6.20A – AudioCodes Mediant 800 MSBG

1. Important Notes

- Check the *SIP 3rd Party Validation Website* for current validation status. The *SIP 3rd party Validation Website can be viewed at:* http://testlab.inin.com
- Unlike other Mediant devices, no INI files will be provided with this document. The Mediant 800 requires two INIs to have a complete configuration. These INI files are interdependent and editing the DATA.INI file is not supported by AudioCodes.
- As this unit is a critical piece of the SIP infrastructure, it is highly recommended that DHCP not be used. A static IP address is the preferred method and is how the unit was configured during validation.
- The M800 will require 3 IP Addresses as a base configuration. One for the WAN interface and two for the internal interfaces (VoIP & Data).
- After a factory reset, the Mediant 800's default configuration has DHCP enabled, and the VOIP & Data IP addresses will be 192.168.0.1 and 192.168.0.2 respectively. The IP Address of the VoIP interface is the address of the Web Interface.
- If a configuration change is made that causes errors, the Mediant 800 will revert to the default IP & DHCP configuration. If this happens connect a PC to the Mediant 800 via crossover cable and undo any changes made.
- The Mediant 800 MSBG has two configuration sections that are controlled by two different INI files. Board.INI contains the VoIP/Gateway configuration. Data.ini contains the Firewall/Routing configuration.
- Any time you see -1 in a configuration this is mean "not configured".
- While this device supports IPv6, IPv4 was used in the certification tests.

2. Vendor Documentation

Documentation can be found on the CD shipped with the Mediant 800.

3. Validated Firmware Version

6.20A.034.004

4. Install

Download the Mediant 800 files form the *3rd Party Validation Website*: http://testlab.inin.com

Contained in the zip file will be the validated version of firmware (.cmp), as well as any supplemental configuration files.

5. Configuration

Methods:

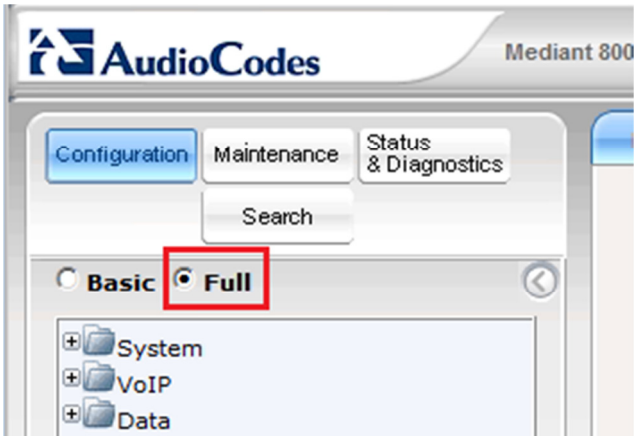
- Manipulation of the supplied .ini file(s), then uploading it via the Web interface.
  - This method is not supported for the Mediant 800. The Mediant 800 requires two separate INI files that are interdependent and modifying the DATA.INI file manually is not supported by AudioCodes. As a result, no INI files have been provided with this document.
- Web Interface
  - This method is the preferred method for all configuration needs.
  - **Please note:** Caution should be exercised and the AudioCodes documentation should always be referenced when using the Web interface configuration option.
- TFTP
  - This method of configuring the Mediant 800 has not been tested.

Contents

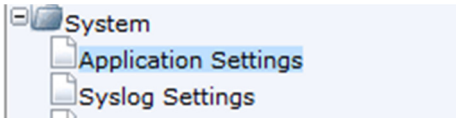
Initial Setup – LAN Settings: 3
Initial Setup – VoIP Settings: 9
Initial Setup – SBC Routing: 23
Advanced Installation – TLS: 26
Advanced Installation – External User Agents: 36

Initial Setup – LAN Settings:

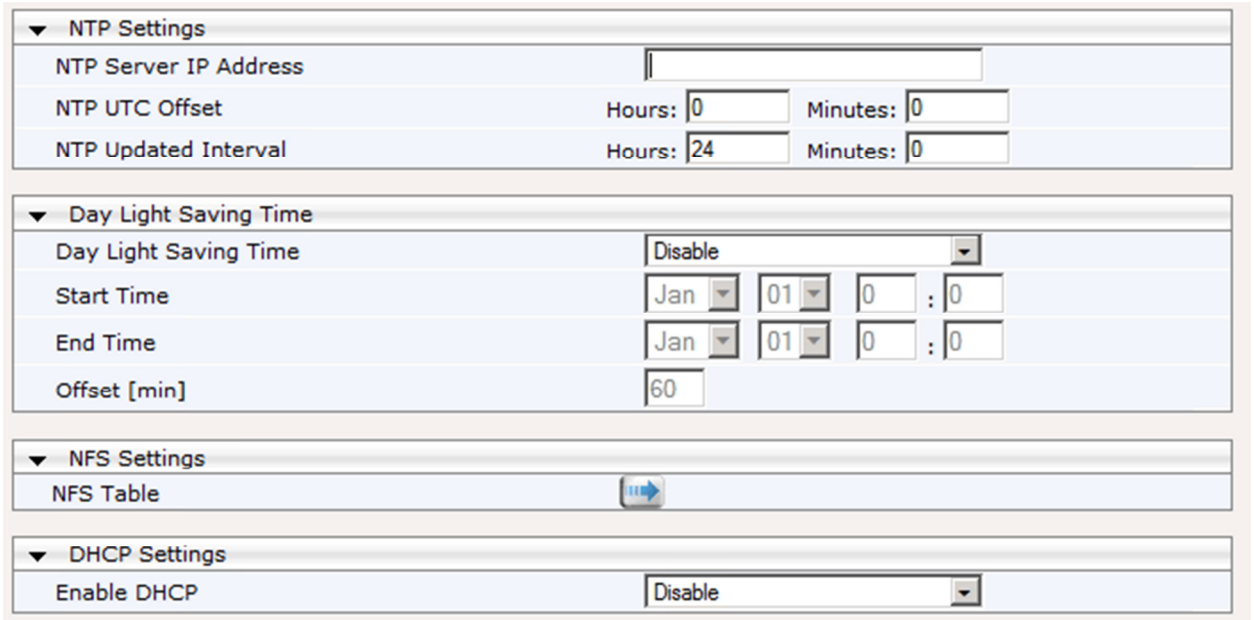
1. Connect a Laptop/Desktop with its NIC configured for DHCP to the Mediant 800 via a crossover cable or a switch
2. Open a browser and navigate to 192.168.0.1 entering the default username and password
   a. User: Admin
   b. Pass: Admin
3. After logging in, always make sure the radio button next to **Full** is selected. Without this radio button selected you do not have access to all the possible configuration options



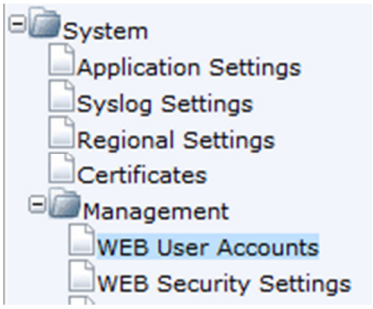
4. Select **System** > **Application Settings**



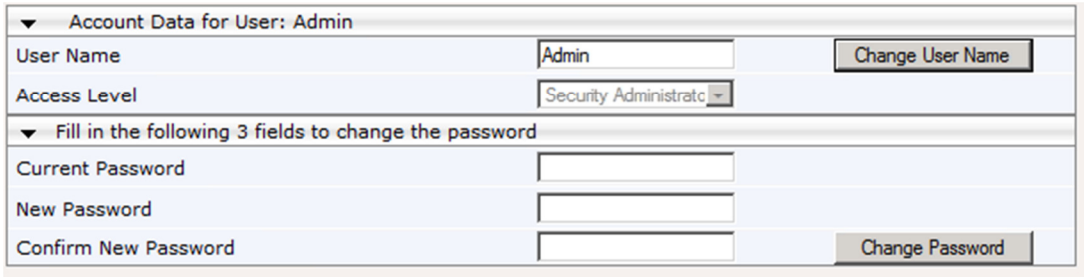
5. Enter the appropriate information for your network



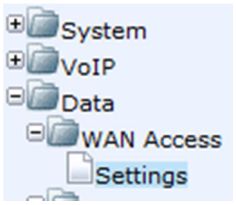
6. Select **System** > **WEB User Accounts**



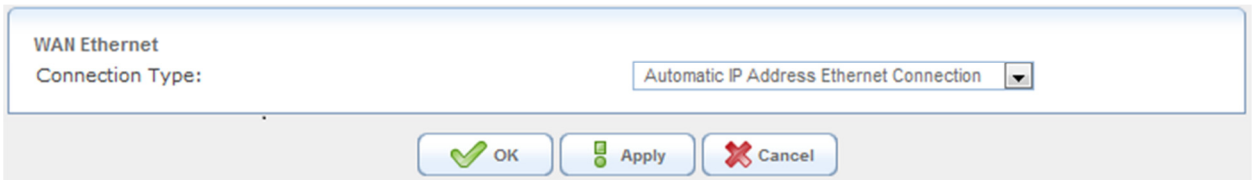
7. Change the Admin user password and, if necessary, the user name



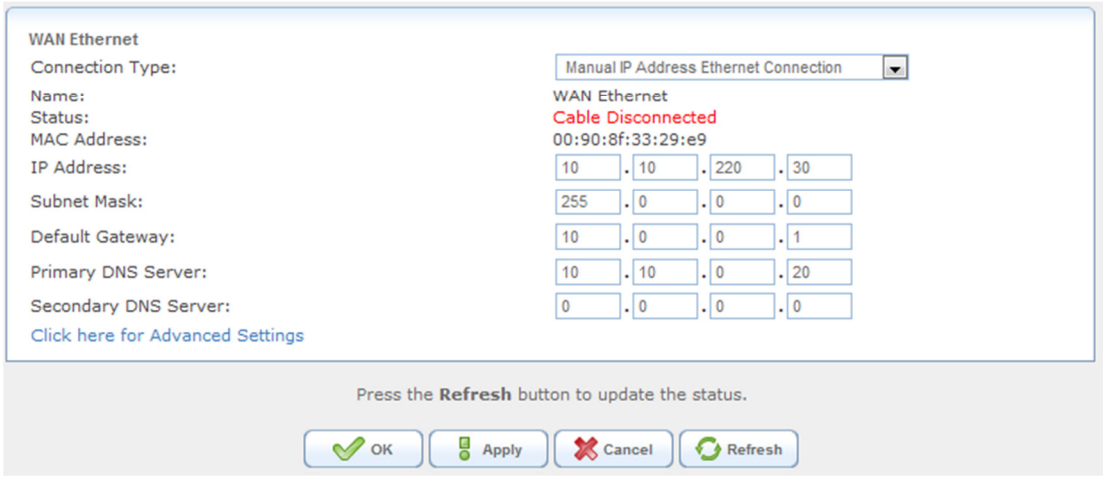
8. Select **Data** > **WAN Access** > **Settings**



9. Change **Connection Type** to **Manual IP Address Ethernet Connection**

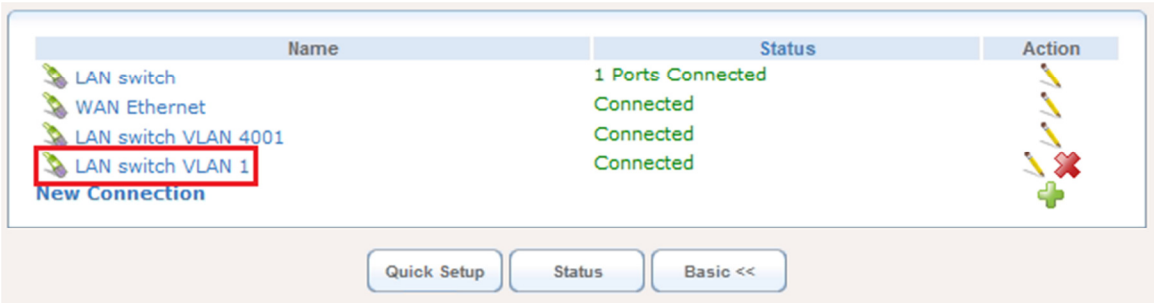


10. Enter the settings necessary to fit your network design.

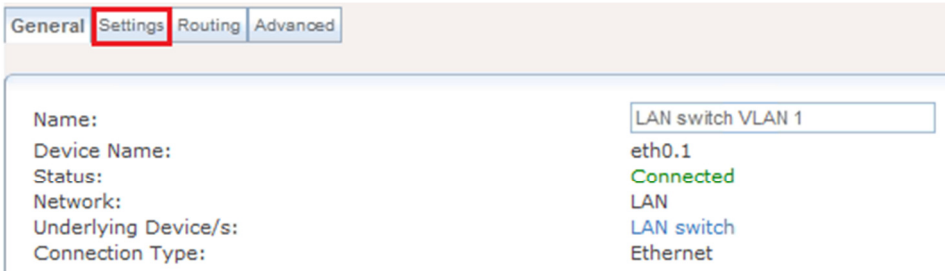


11. Select **Data** > **Data System** > **Connections**

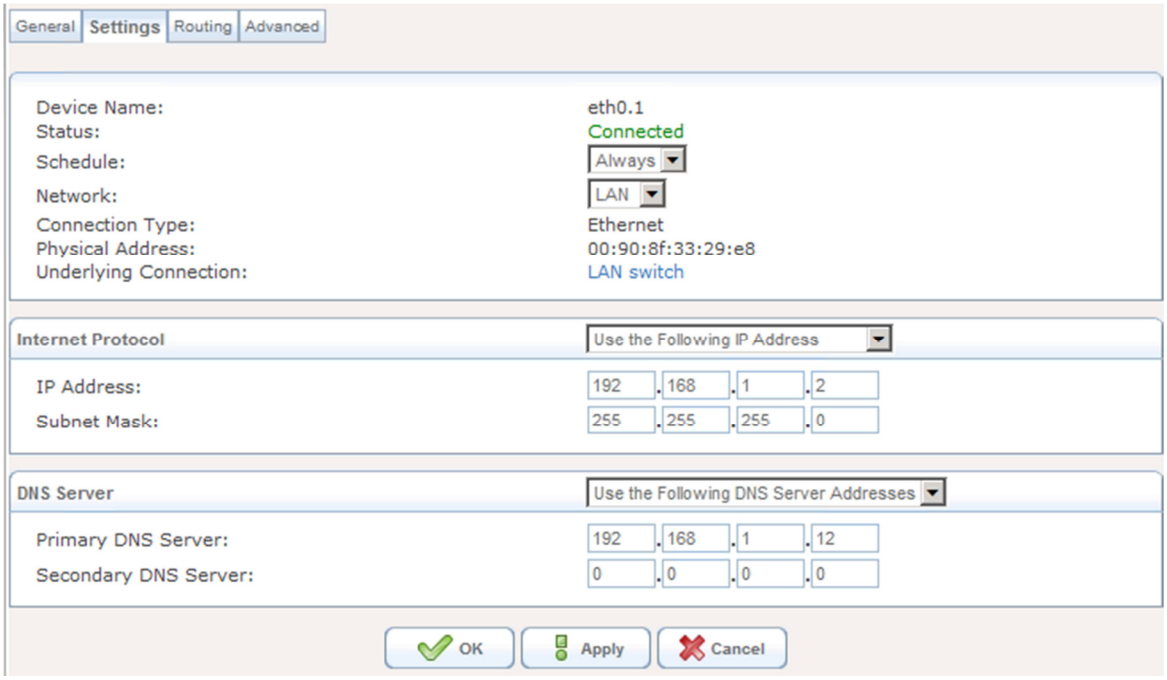
12. Select **LAN Switch VLAN 1**



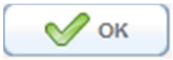
13. Select **Settings**



14. Enter the settings necessary to fit your network design.

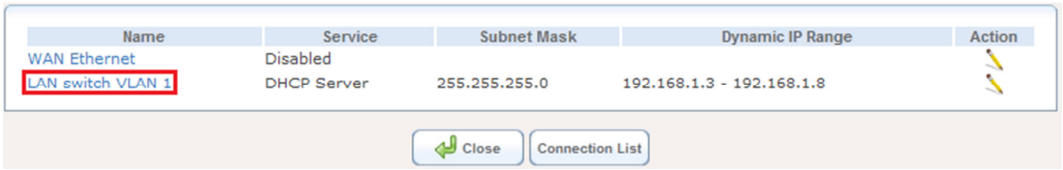


15. Click **OK** on this and the next page

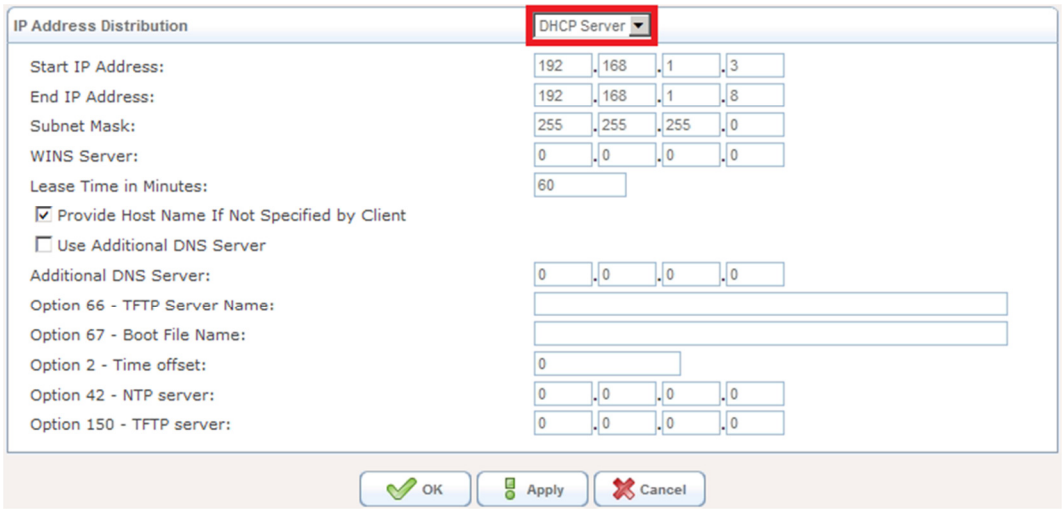


16. Select **Data** > **Data Services** > **DHCP Server**

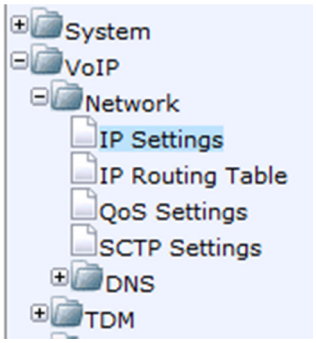
17. Select **LAN switch VLAN 1**



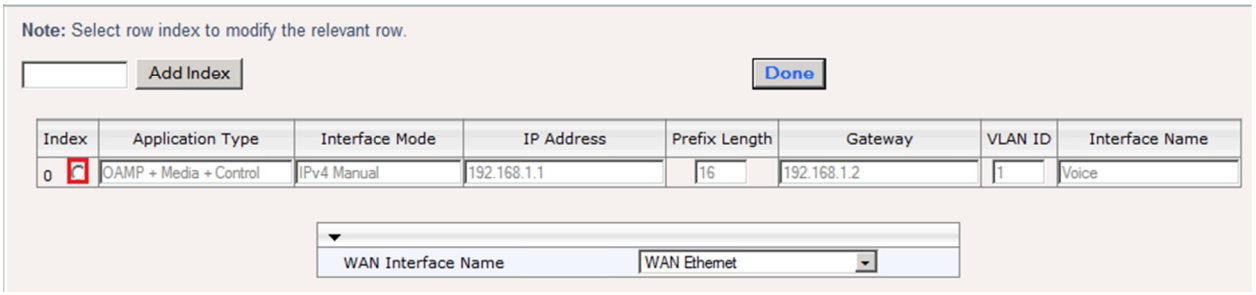
18. If you do not wish to use the Mediant 800's DHCP server then change the highlighted (see below) drop down to **Disabled** and click **OK**. Otherwise, modify the settings to fit your network design.


IP Address Distribution
DHCP Server
Start IP Address: 192.168.1.3
End IP Address: 192.168.1.8
Subnet Mask: 255.255.255.0
WINS Server: 0.0.0.0
Lease Time in Minutes: 60
Provide Host Name If Not Specified by Client
Use Additional DNS Server
Additional DNS Server: 0.0.0.0
Option 66 - TFTP Server Name:
Option 67 - Boot File Name:
Option 2 - Time offset: 0
Option 42 - NTP server: 0.0.0.0
Option 150 - TFTP server: 0.0.0.0
OK
Apply
Cancel

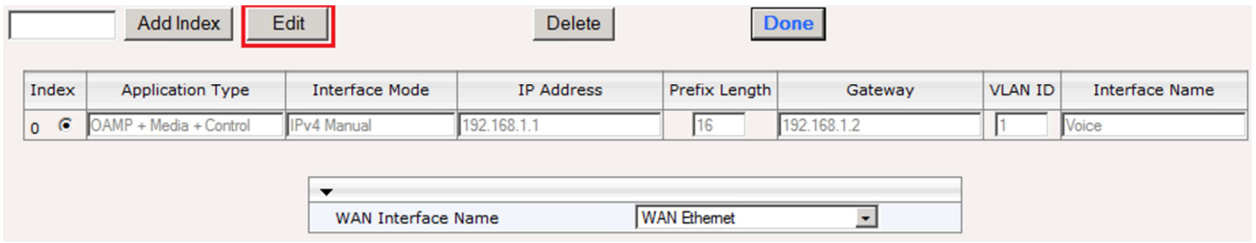
19. Select **VoIP** > **Network** > **IP Settings**



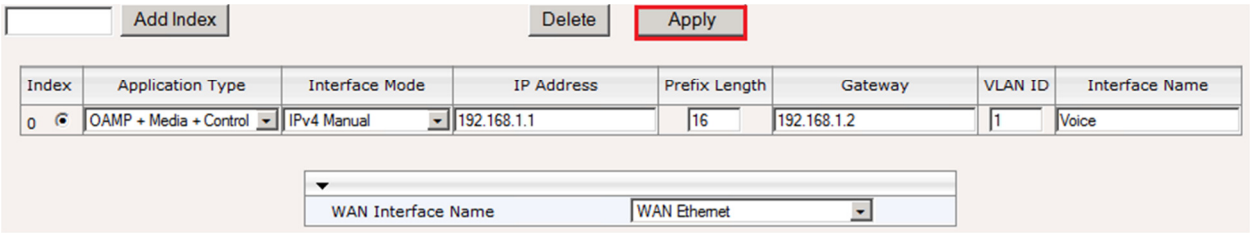
20. Click the radio button next to **Index 0**



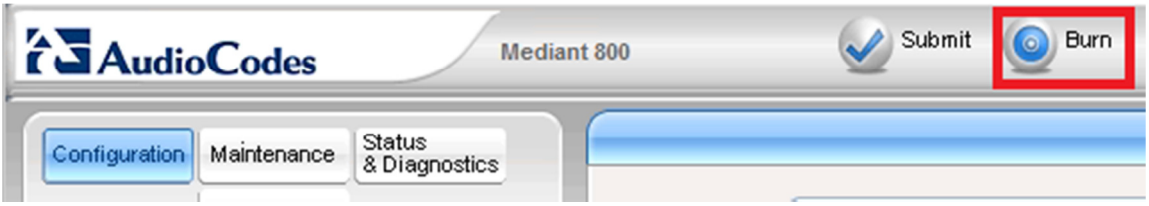
21. Click the **Edit** button that appears above the IP settings table



22. Enter the information necessary to fit your network design. Also ensure that the **WAN Interface Name** has the proper Interface selected in the drop down. Click **Apply**.



23. Click **Burn** & then **Yes** on the following dialog prompt.



24. Now that the configuration has been saved to memory and the Mediant 800 is configured to be on your LAN, put it in place and we'll continue in the next section with the configuration.

Initial Setup – VoIP Settings:

In this section we'll be configuring the Mediant 800 to accept & route calls. The Mediant 800 uses an organizational structure where groups of settings are contained in a Signaling Media Realm (SRD). For further description please see the **Configuring SRD Table** section of the **Mediant 800 MSBG User's Manual**.

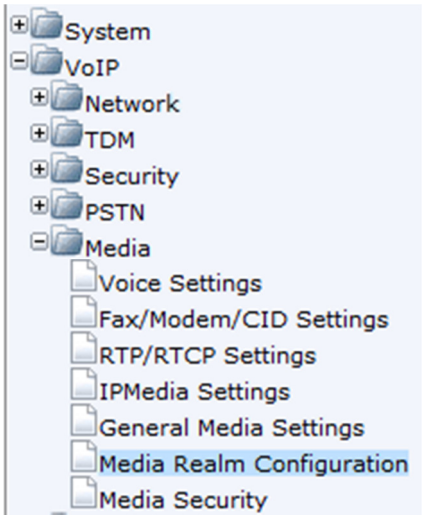
There are several pieces that will need to be configured to construct the SRD. They are:

1) Media Realm
2) IP Group
3) IP Profile
4) Proxy Set

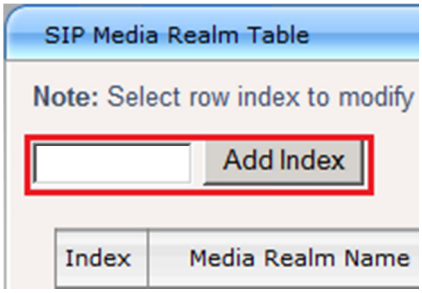
We will also be configuring the VoIP Interface settings (ports, etc), and Routing. The Routing Table is where SRDs & IP Groups are used to ease the configuration of routing between networks.

After the Mediant 800 has been connected to your LAN and you have established connectivity, continue below. The MSBG has built in diagnostic tools (PING, ARP, & Traceroute) you can use to verify successful configuration. They are located under **Status & Diagnostics** > **Data Status** > **Diagnostics**.

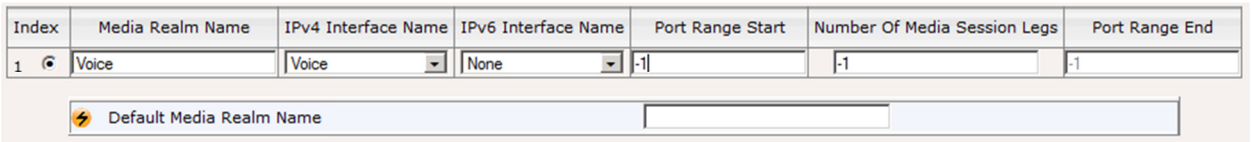
1. Select **VoIP** > **Media** > **Media Realm Configuration**



3. The default configuration has no media realms configured. You will need at least two realms configured. One for WAN and one for Voice. Enter a number next to Add Index and click Add. For the purposes of this document, we will be considering Voice indexes to be between 1 & 10 and WAN indexes to be between 11 & 20.

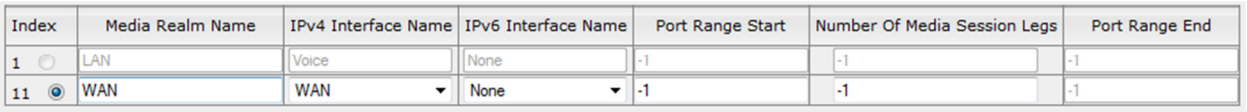


4. Enter the following settings:
   a. **Media Realm Name**: Voice
   b. **IPv4 Interface Name**: Voice
   c. **Port Range Start**: This is as needed.
      i. If you configure **Port Range Start**, then **Port Range End** will be automatically calculated. Also, you will need to configure **Port Range Start** for all other media realms. These port ranges cannot overlap.
   d. **Number of Media Session Legs**: This will limit the number of active calls the **Media Realm** will allow. -1 = Unlimited



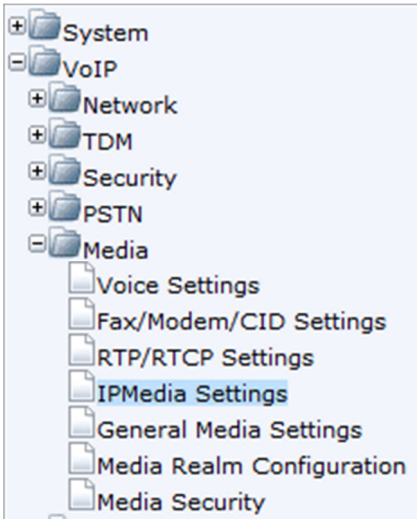
5. Click **Apply**. A dialog box appears telling you that you've configured and offline parameter. Ignore this for now as we will be rebooting later.

6. Add the WAN Media realm following the same steps.

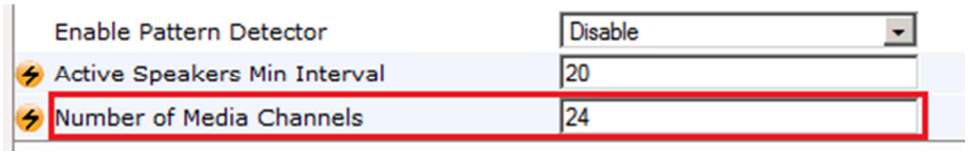


7. Click **Apply**. A dialog box may appear telling you that you've configured and offline parameter. Ignore this for now as we will be rebooting later.

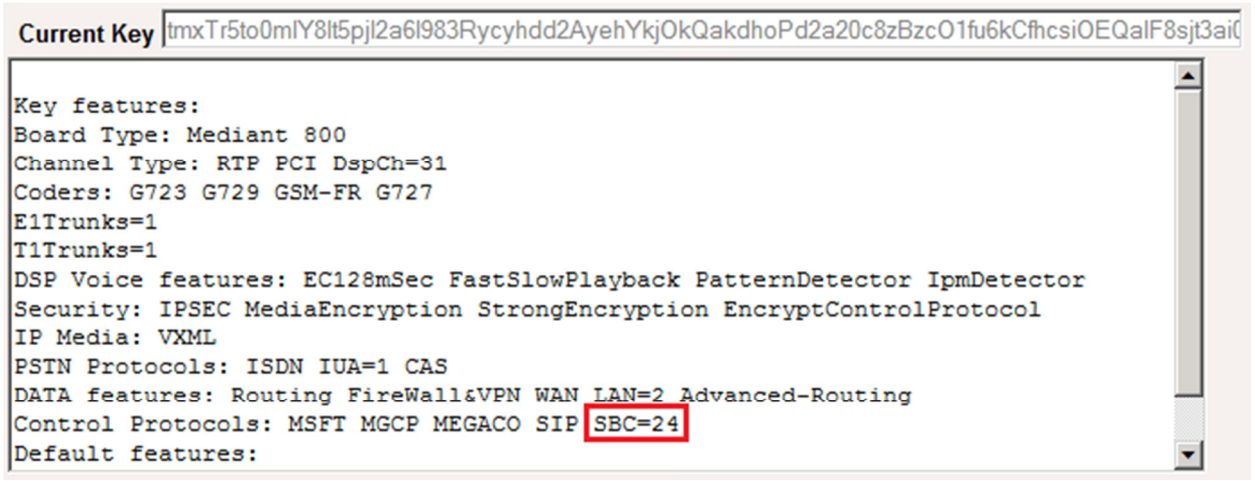
8. Select **VoIP** > **Media** > **IPMedia Settings**



9. Enter in the **Number of Media Channels** that were purchased with your feature key.

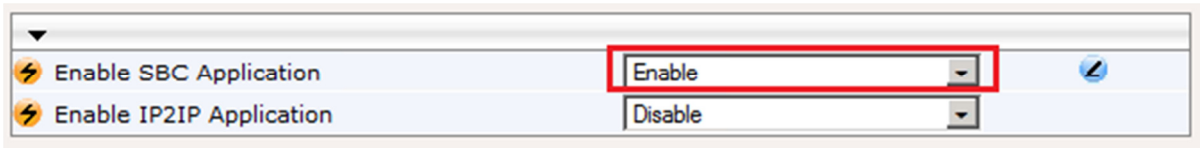


Note: If you do not know the number, check in **Maintenance** > **Software Update** > **Software Upgrade Key** and on the right hand side look for the following value:



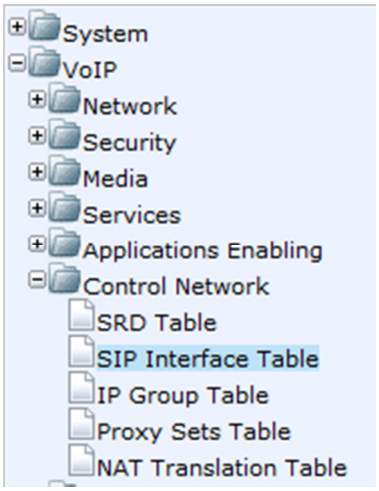
10. Select **VoIP** > **Applications Enabling** > **Applications Enabling**

11. Change **Enable SBC Application** to **Enable**

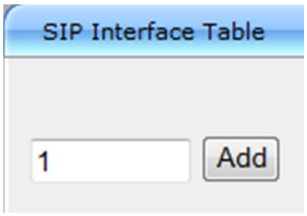


12. Click **Submit**

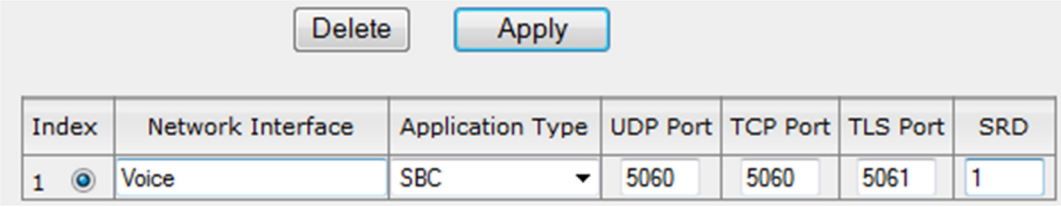
13. Select **VoIP** > **Control Network** > **SIP Interface Table**



14. Enter 1 in the box next to **Add** and then click **Add**.

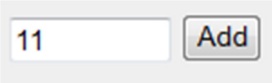


15. Enter a Network Interface name, SIP Ports, SRD, and choose an application type (SBC) for the SIP Interface. Click **Apply**.

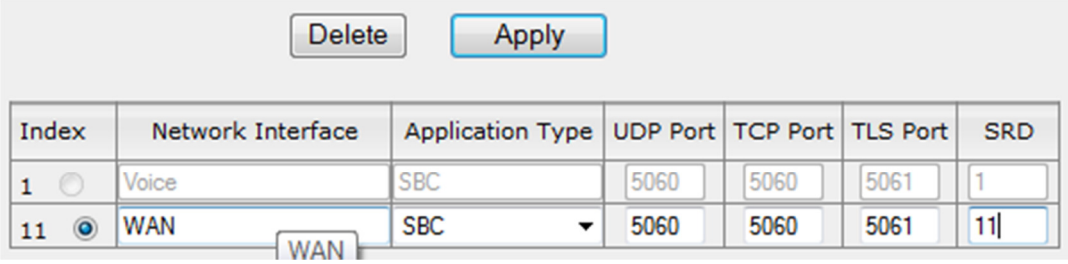


Note: The Network Interface Name has to match, precisely, the name given to the VoIP Interface in **VoIP** > **Network** > **IP Settings**.

16. Enter 11 in the box next to **Add** and then click **Add**.



17. Enter a Network Interface name, SIP Ports, SRD, and choose an application type (SBC) for the SIP Interface. Click **Apply**.

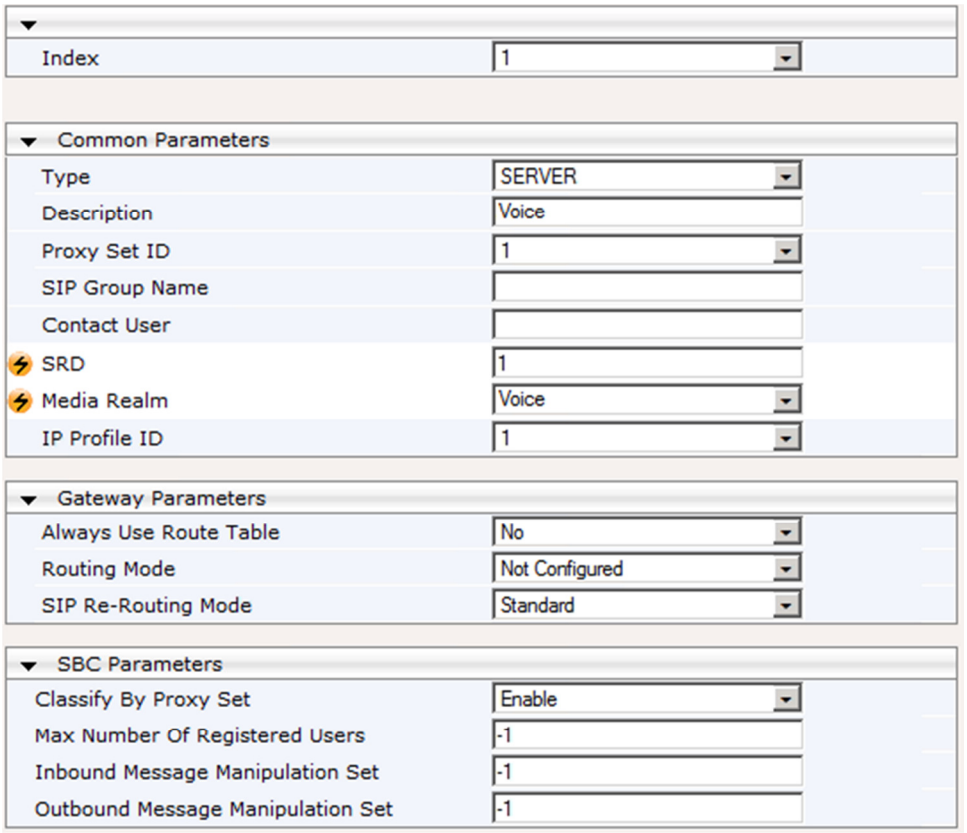


Note: WAN is the default Network Interface name for the WAN port. It is not recommended to try changing this.

18. Select **VoIP** > **Control Network** > **IP Group Table**

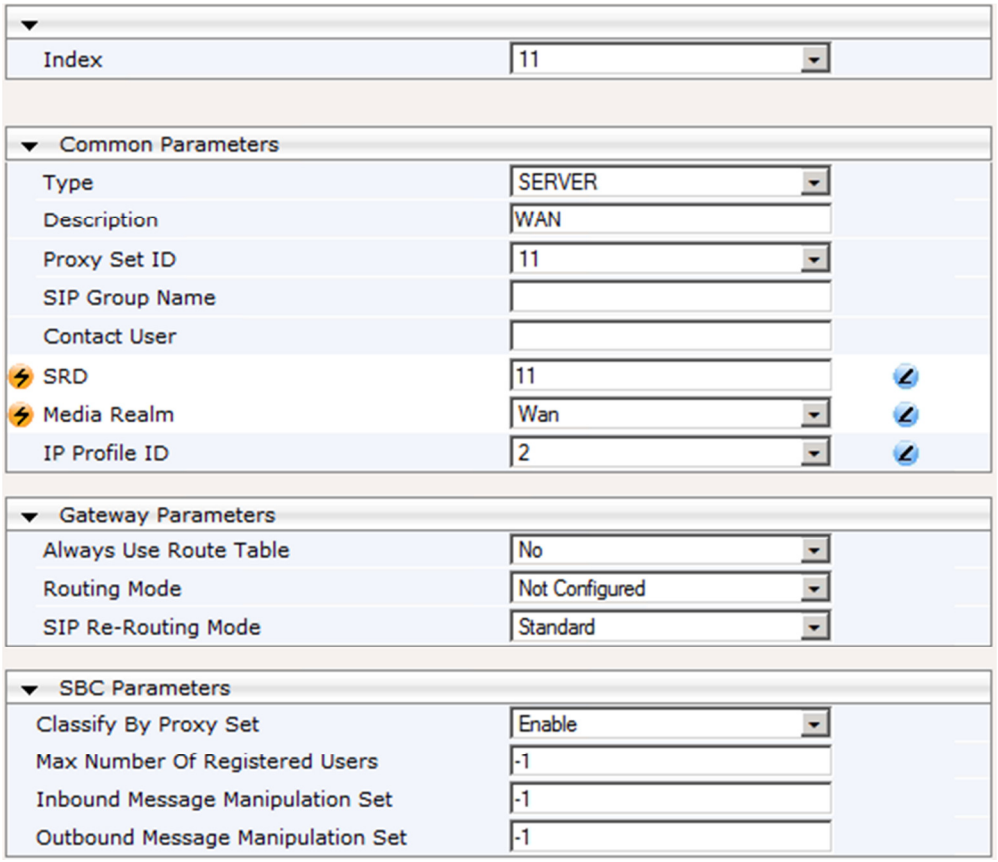
19. In the **IP Group Table** select and/or enter the following values for the LAN & Wan Groups clicking **Submit** when settings are entered.
    a. LAN group:

Index: 1
Type: Server
Description: Voice
Proxy Set ID: 1
SIP Group Name: <Blank>
Contact User: <Blank>
SRD: 1
Media Realm: Voice
IP Profile ID: 0
Always Use Route Table: No
Routing Mode: Not Configured
SIP Re-Routing Mode: Standard
Classify By Proxy Set: Enable
Max Number of Registered Users: -1
Inbound Message Manipulation Set: -1
Outbound Message Manipulation Set: -1



b. WAN Group:

Index: 11
Type: Server
Description: WAN
Proxy Set ID: 11
SIP Group Name: <Blank>
Contact User: <Blank>
SRD: 1
Media Realm: WAN
IP Profile ID: 0
Always Use Route Table: No
Routing Mode: Not Configured
SIP Re-Routing Mode: Standard
Classify By Proxy Set: Enable
Max Number of Registered Users: -1
Inbound Message Manipulation Set: -1
Outbound Message Manipulation Set: -1



20. Select **VoIP** > **Control Network** > **Proxy Sets**

21. You will need to create two proxy sets, one for the IC Server(s) and one for your WAN Side end point(s). Select and/or enter the following values for the LAN & Proxy Sets clicking **Submit** when settings are entered.

Continues on next page.

a. LAN:

Proxy Set ID: 1

Proxy Address

Enter the IP of the Primary IC Server in the first line and, if applicable, the IP of the Backup IC Server in the second line. Choose the appropriate **Transport Type** for each.

Note: While not strictly necessary, it is recommended to put the appropriate SIP communications port on end of the IC Servers' IP Addresses.

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

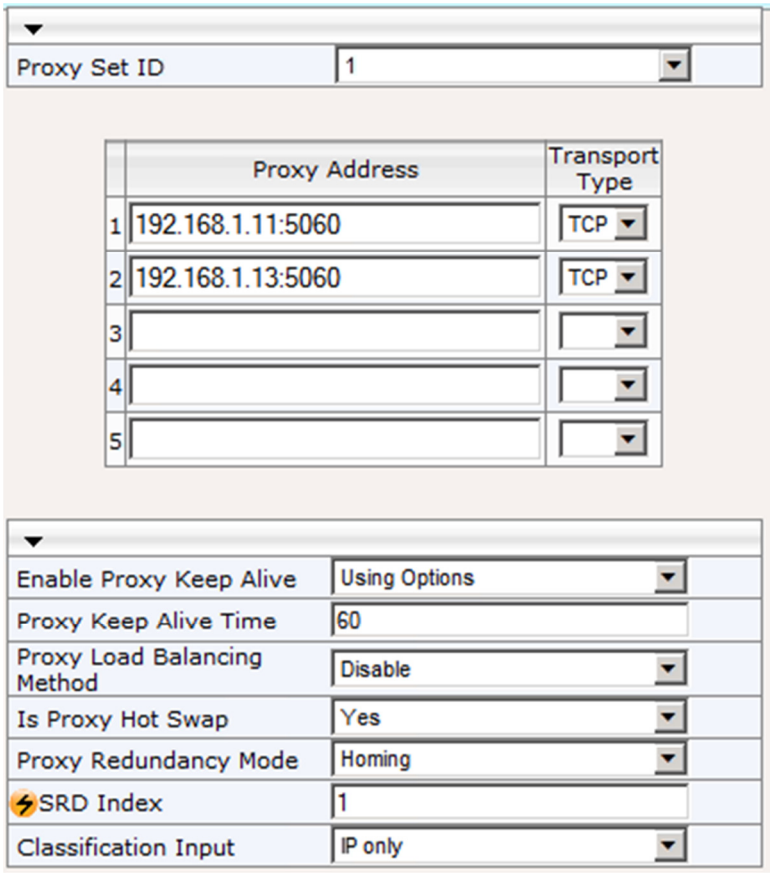
Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: Yes

Proxy Redundancy Mode: Homing

SRD Index: 1

Classification Input: IP Only



b. WAN:

Proxy Set ID: 11

Proxy Address

If you have redundant carrier endpoints enter their IPs here. Else, enter the IP of your carrier. Choose the appropriate **Transport Type**.

Note: While not strictly necessary, it is recommended to put the appropriate SIP communications port on the IP Address(es).

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

Proxy Load Balancing Method:

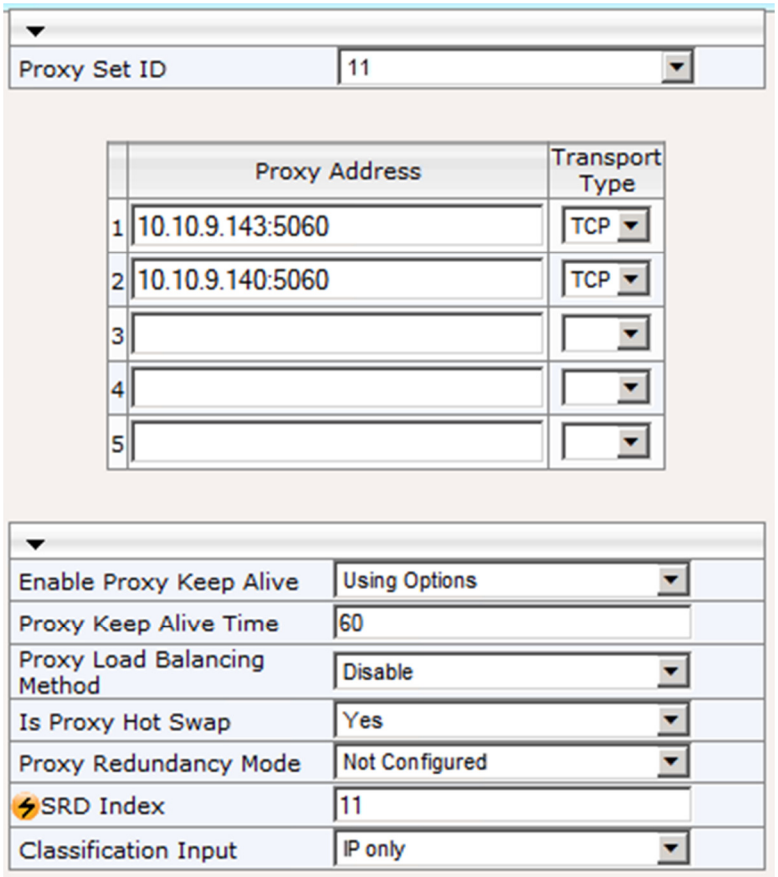
If your carrier allows for load balancing, pick the appropriate method.

Is Proxy Hot Swap: Yes

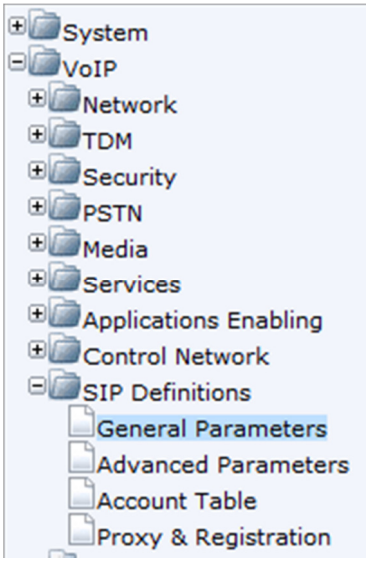
Proxy Redundancy Mode: Homing

SRD Index: 11

Classification Input: IP Only



22. Select **VoIP** > **SIP Definitions** > **General Parameters**



23. There are many different combinations of settings you can use here. The main things that need configured are:
    Enable Early Media: Configure as needed
    Fax Signaling Method: T.38 Relay
    SIP Transport Type: Configure as needed
    SIP UDP Local Port: Same as Voice SIP Interface
    SIP TCP Local Port: Same as Voice SIP Interface
    SIP TLS Local Port: Same as Voice SIP Interface
    Enable Sips: Please see the section on Enabling TLS.
    SIP Destination Port: Matches protocol for **SIP Transport Type**
24. Once your changes are complete, click **Submit**

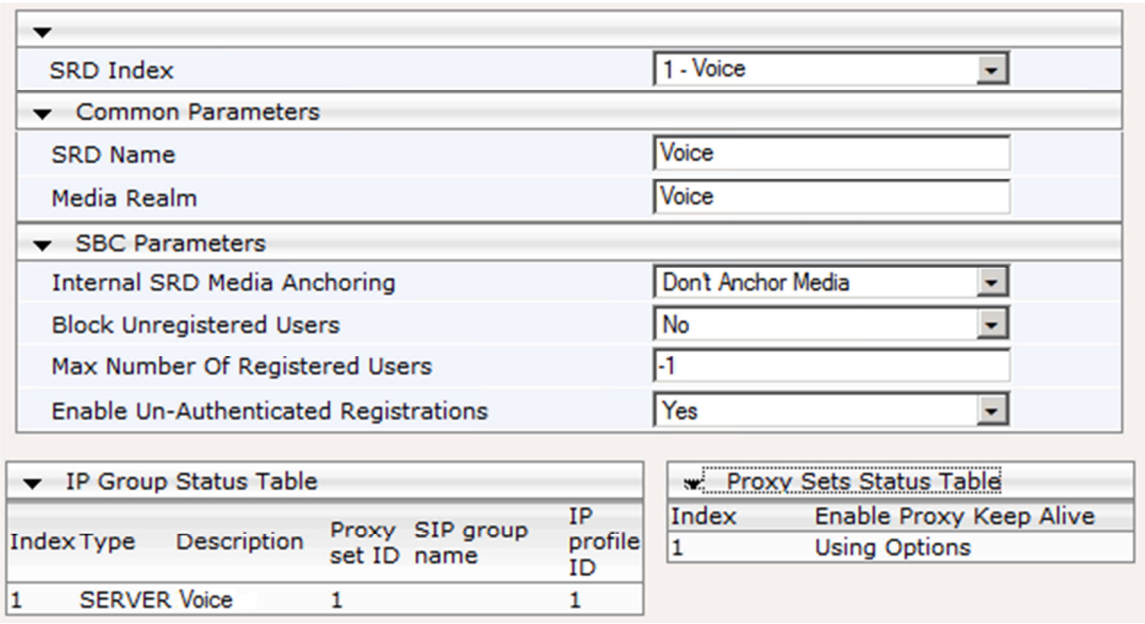
25. Select **VoIP** > **Coders and Profiles** > **IP Profile Settings**

26. Here you can configure various settings to handle variations on the default SIP parameters. You then assign these Profiles to their respective IP Groups to override the default SIP Parameters.

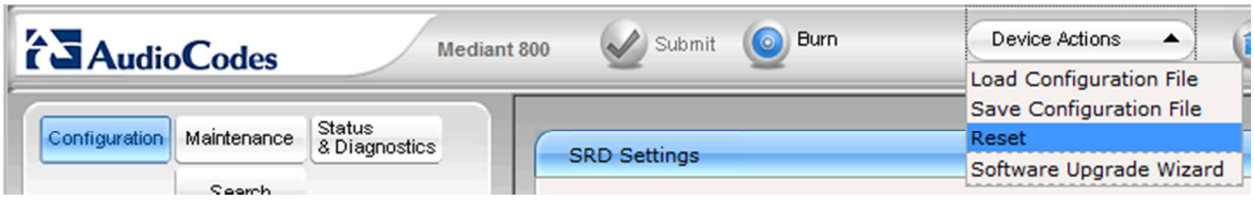
    These profiles can be used to handle:
    a. Differences in DSCP from one network to another
    b. If one network uses SRTP and another uses RTP if Media Security is Enabled
    c. If one network uses T.38 Relay and another does not allow faxing
    d. If you set up Coder Groups you can assign them to the IP Profile and then assign the IP Profile to the proper IP Groups.
    e. Etc.
27. Once your configurations are complete, press **Submit** and, if necessary, assign them to the proper **IP Groups**.

28. Select **VoIP** > **Control Network** > **SRD Table**

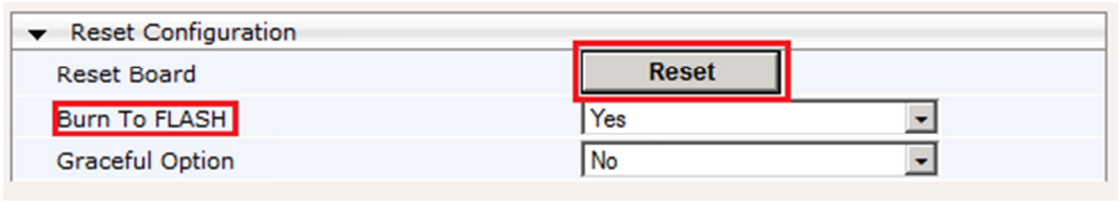
29. Select **SRD Index**: 1 – Not Exist
30. Expand all sections by clicking the ^s next to their names. Configure as follows:
    SRD Name: Voice
    Media Realm: Voice
    Internal SRD Media Anchoring: Don't Anchor Media
31. After you have clicked **Submit** the SRD should look like this:



32. Select **SRD Index**: 11 – Not exist
33. Expand all sections by clicking the ^s next to their names. Configure as follows:
    SRD Name: WAN
    Media Realm: WAN
    Internal SRD Media Anchoring: Don't Anchor Media
34. Select **Device Actions** > **Reset**



35. Ensure **Burn to Flash** is set to **Yes** and then click **Reset**

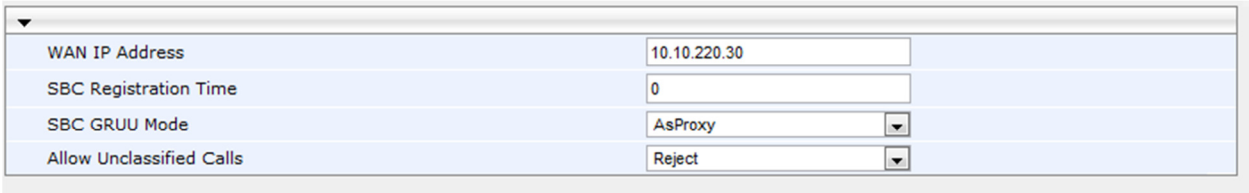


Initial Setup – SBC Routing:

Now that the SRDs & IP Groups have been configured we can move on to configuring routing between IP Groups. For more details see the Configuring **SBC IP-to-IP Routing** section of the **Mediant 800 MSBG SIP User's Manual**.

1. Select **VoIP** > **SBC** > **General Settings**

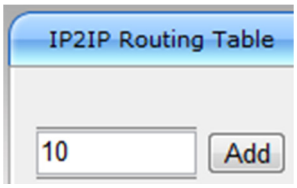
2. Enter the WAN IP address configured earlier in the **WAN IP Address** field



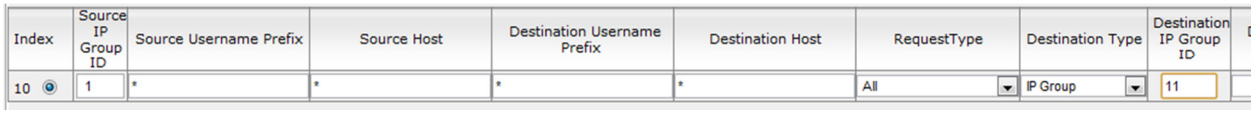
3. Click **Submit**

4. Select **VoIP** > **SBC** > **Routing SBC** > **IP to IP Routing Table**

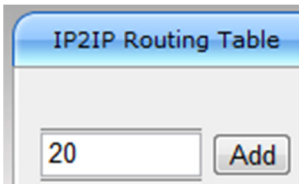
5. Enter a 10 in the text box next to Add. Click **Add**



6. Enter the following settings:
   Source IP Group ID: 1
   Destination IP Group ID: 11



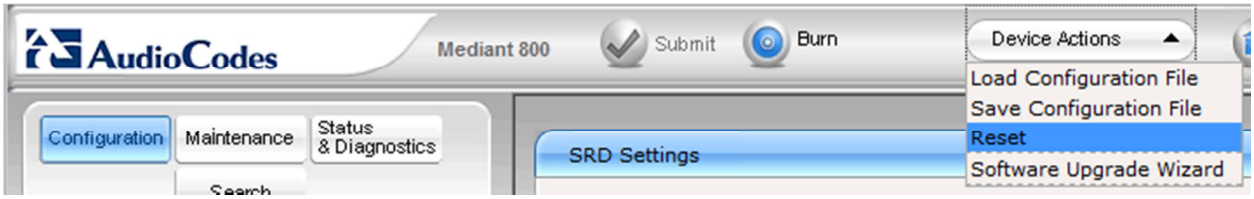
7. Click **Apply**
8. Enter 20 in the text box next to Add. Click **Add**



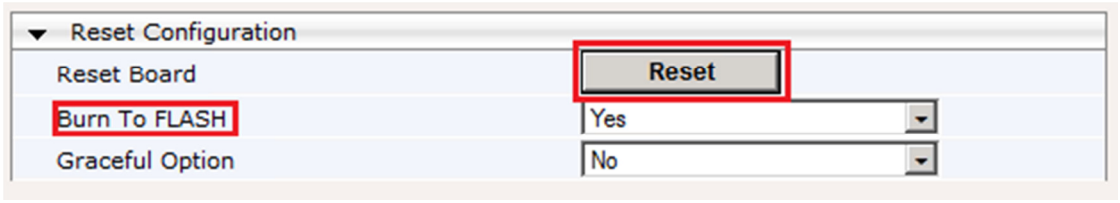
9. Enter the following settings:
   Source IP Group ID: 11
   Destination IP Group ID: 1

Index	Source IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	RequestType	Destination Type	Destination IP Group ID
10	1	*	*	*	*	All	IP Group	11
20	11	*	*	*	*	All	IP Group	1

10. Click **Apply**
11. Select **Device Actions** > **Reset**



12. Ensure **Burn to Flash** is set to **Yes** and then click **Reset**

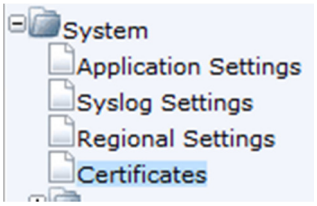


Advanced Installation – TLS:

Please note:

- If you're traffic is moving between TLS & Non-TLS networks it is very important to create two IP Profiles, one for NON-TLS and the other for TLS.

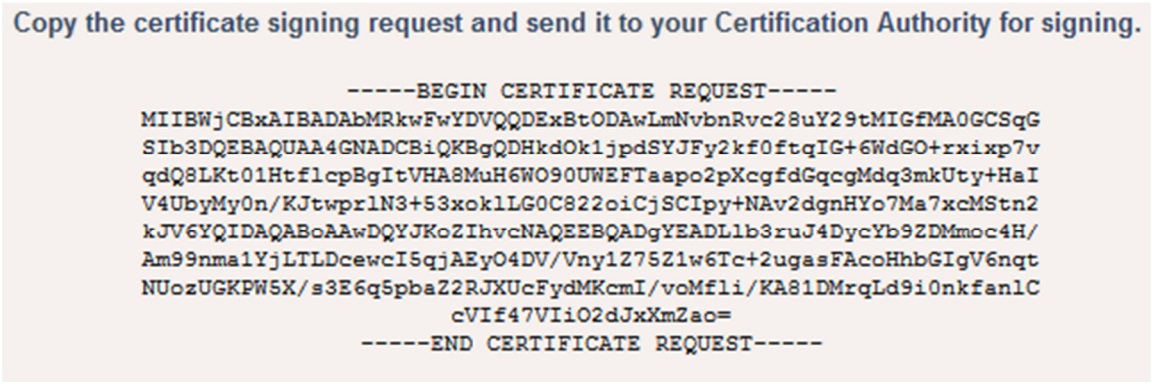
1. Select **System** > **Certificates**



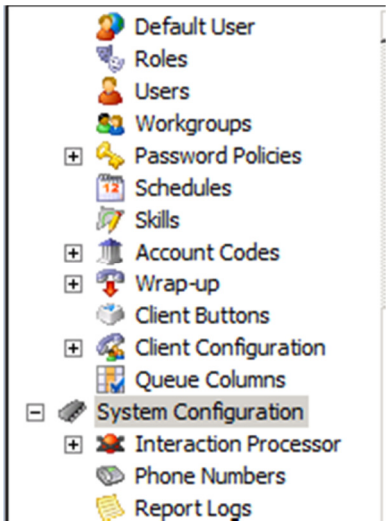
2. Enter the FQDN of the Mediant 800 gateway in **Subject Name**. Click **Generate CSR**

Note: It is necessary to use a **Subject Name** that is resolvable by all network elements, both Internal and External.

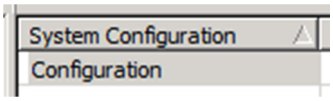
3. Copy all text from **-----BEGIN CERTIFICATE REQUEST-----** to **----- END CERTIFICATE REQUEST-----** including the section headers.



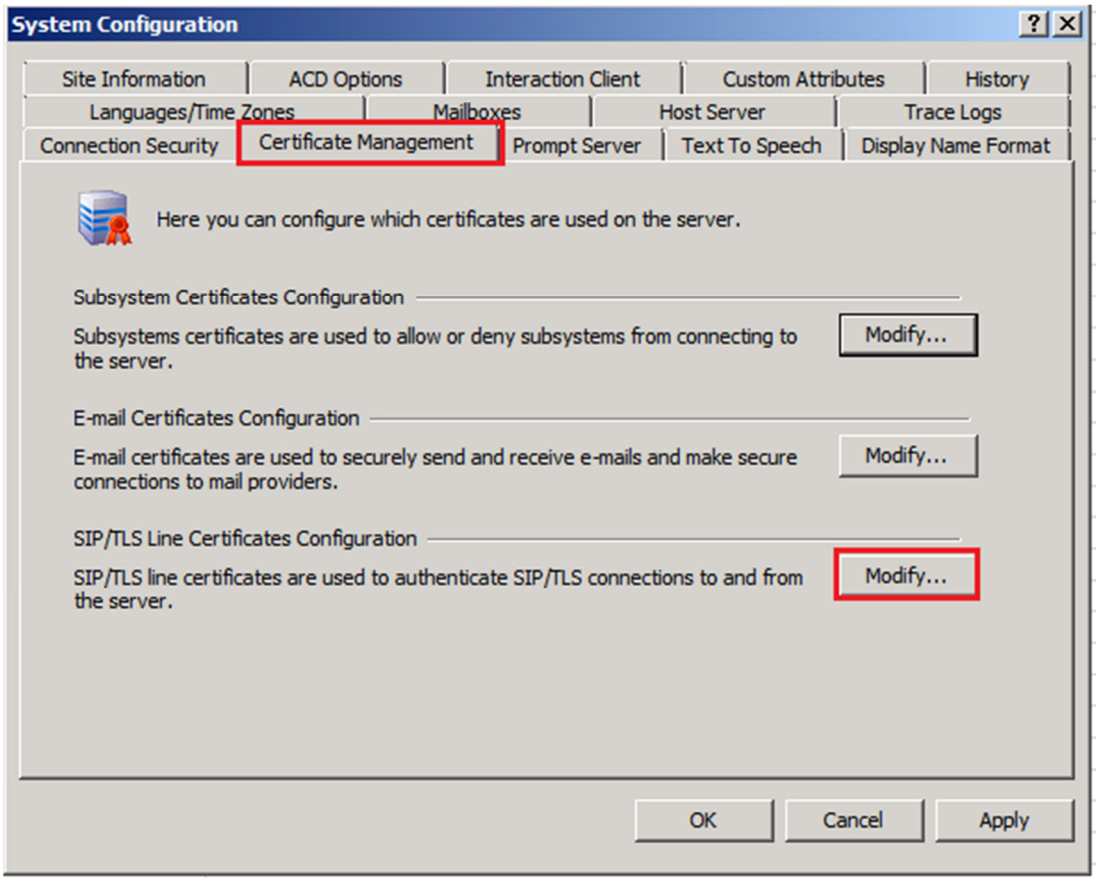
4. Open **Interaction Administrator** and navigate to the **System Configuration** container:



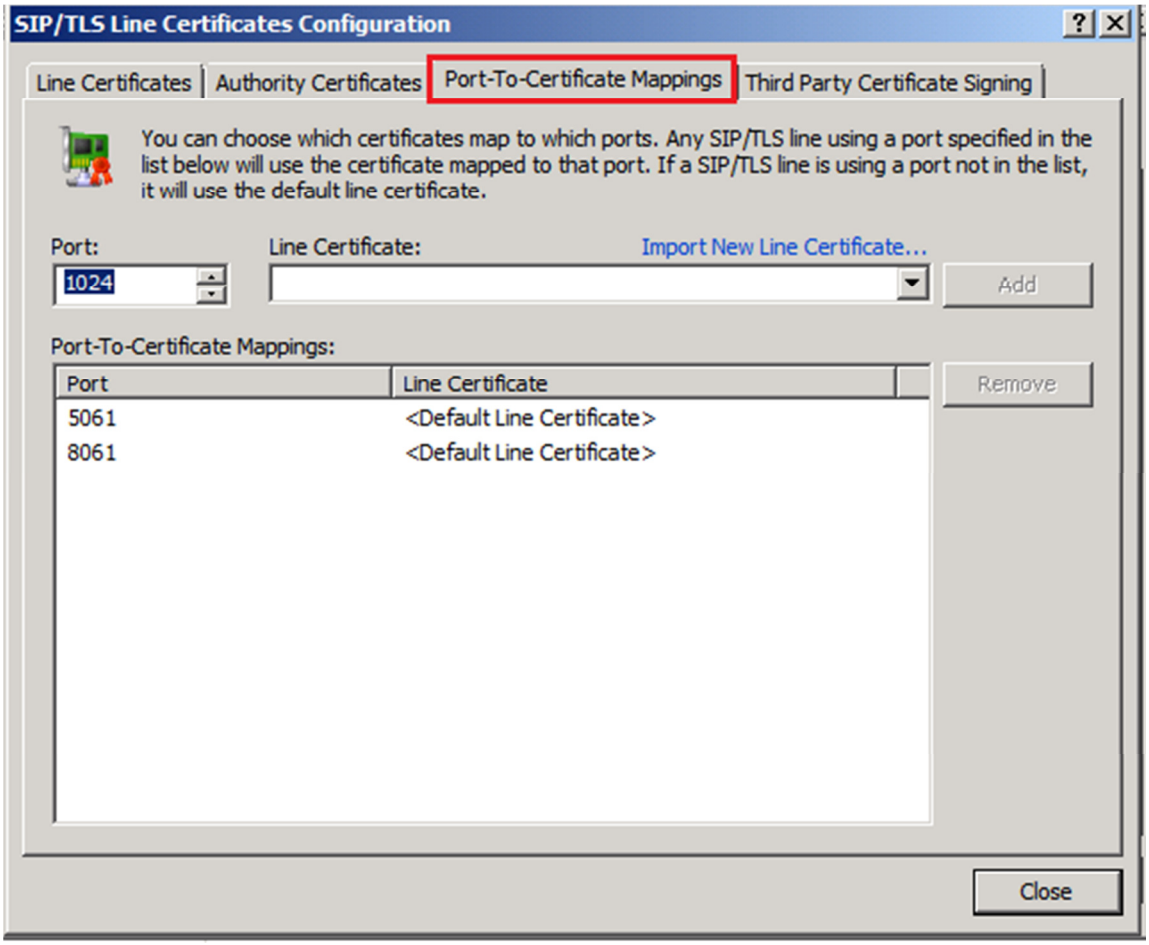
5. On right hand side double-click on **Configuration**



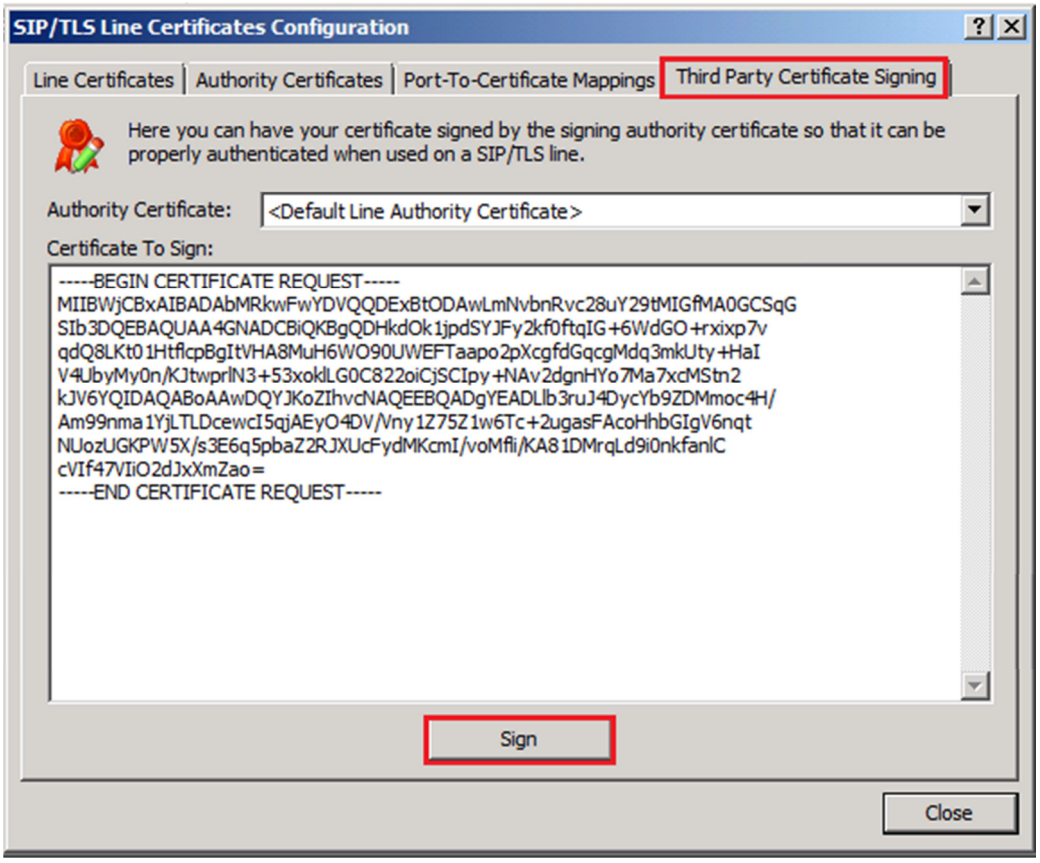
6. Open the **Certificate Management** tab and click the **Modify…** button for the **SIP/TLS Line Certificates Configuration**



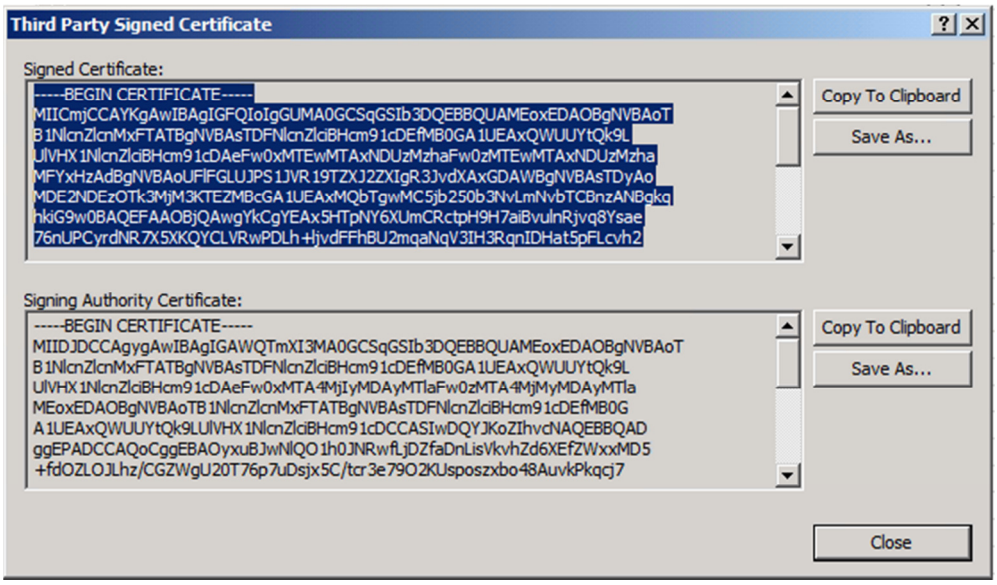
7. Click the **Port-To-Certificate Mappings** tab.
8. Remove all entries in the **Port-To-Certificate Mappings** box
9. Enter 5061 in the **Port** input box and choose **<Default Line Certificate>** in the **Line Certificate** drop down.
10. Click **Add** and then do the same for **8061**.



12. Click **Third Party Certificate Signing**
13. Paste the CSR generated at step 3 into the **Certificate to Sign** input box.
14. Click **Sign**



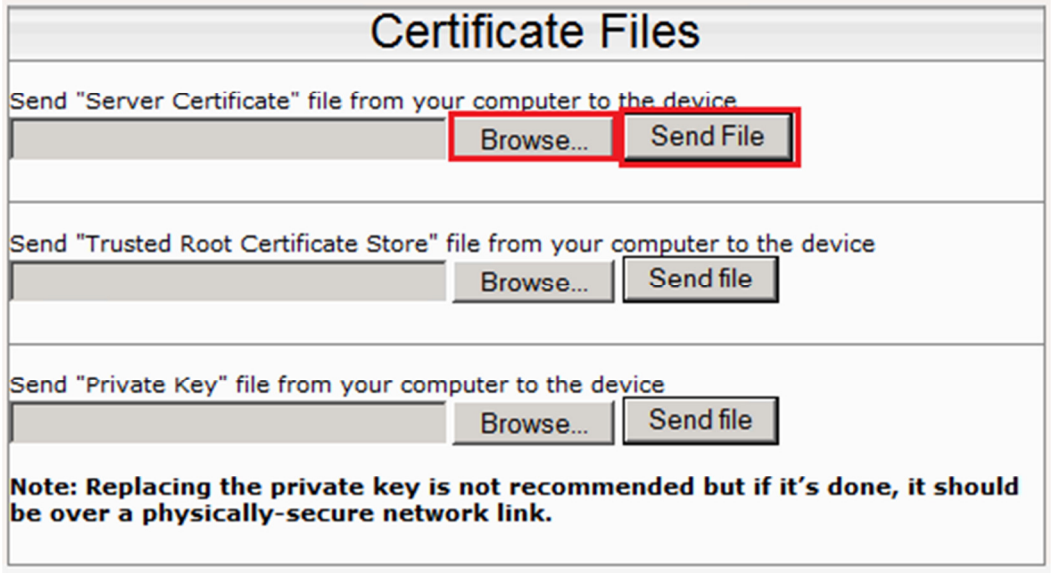
15. You will need to save both the **Signed** and **Signing Authority** certificates for importing to the Mediant 800.



16. Click **Save As…** and save both certificates then return to the Mediant 800 Web Interface.
17. Return to **System** > **Certificates** and click **Browse…** under the **Trusted Root Certificate Store** section of **Certificate Files**. Once you've selected the **Signing Authority Certificate** you saved from Interaction Administrator, click **Send File**

Certificate Files
Send "Server Certificate" file from your computer to the device
Browse...
Send File
Send "Trusted Root Certificate Store" file from your computer to the device
Browse...
Send file
Send "Private Key" file from your computer to the device
Browse...
Send file
Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

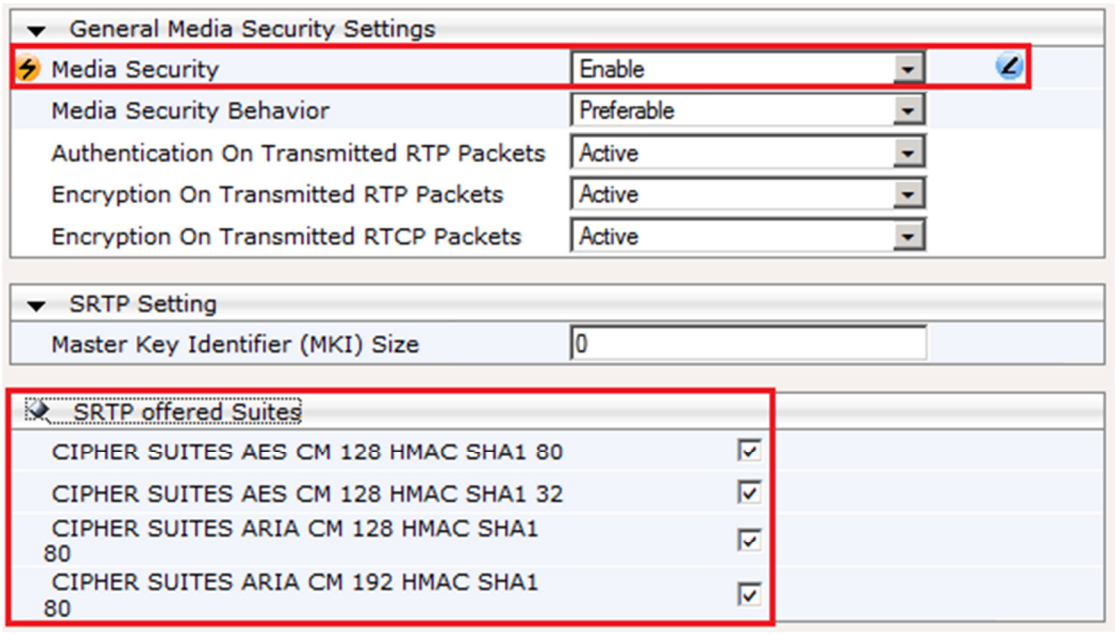
18. Once the file has been uploaded do the same for **Server Certificate**.


Certificate Files
Send "Server Certificate" file from your computer to the device
Browse...
Send File
Send "Trusted Root Certificate Store" file from your computer to the device
Browse...
Send file
Send "Private Key" file from your computer to the device
Browse...
Send file
Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Note: It is exceedingly important that you upload the certificates in that order.

19. Once the file has been uploaded go to **VoIP** > **Media** > **Media Security**

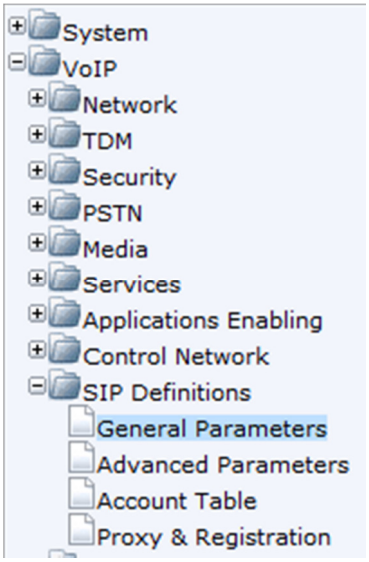
20. Change **Media Security** to **Enable** and put a check next to all applicable cipher suites in **SRTP offered Suites**



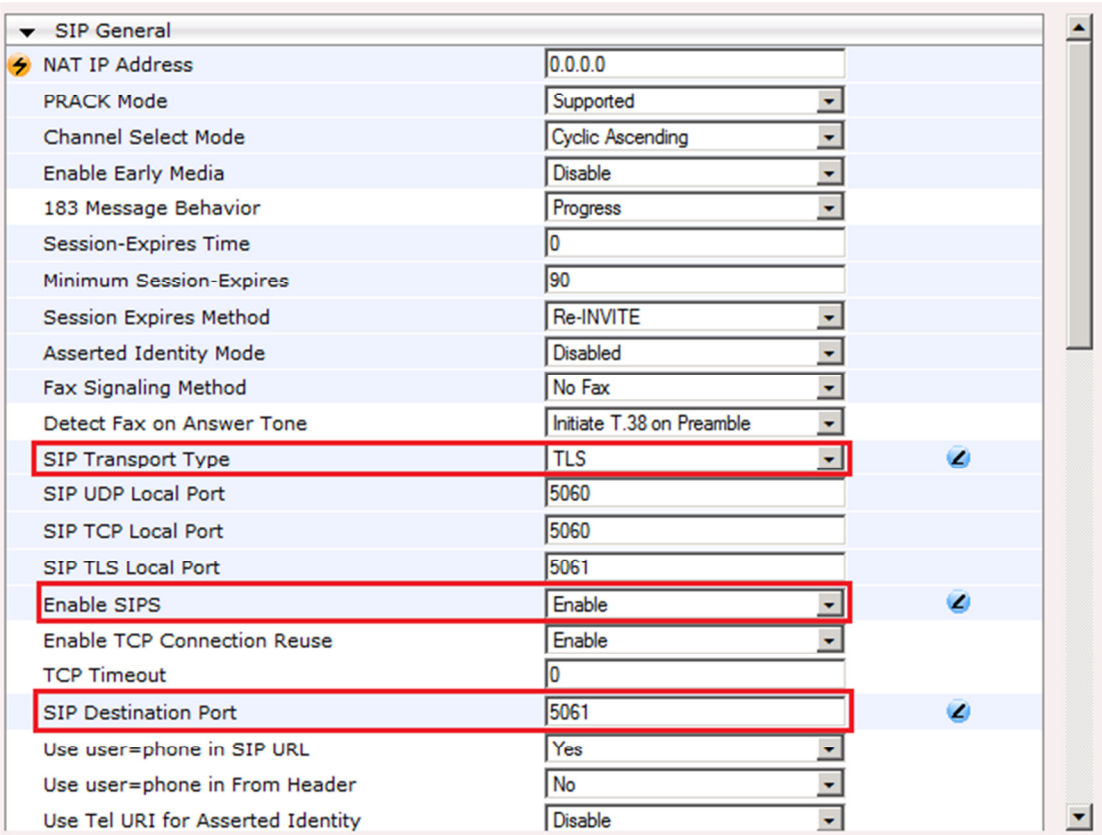
21. Click **Submit**

22. Click OK on the following prompt notifying you of the offline parameter change.

23. Select **VoIP** > **SIP Definitions** > **General Parameters**

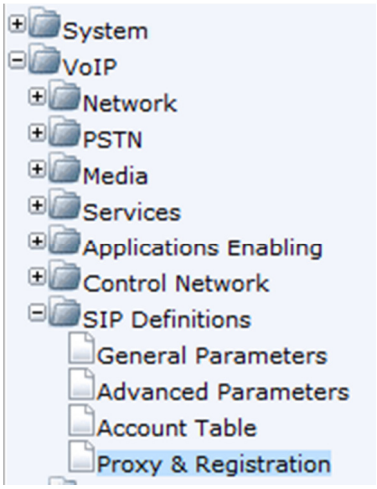


24. Change the following settings:
SIP Transport Type: TLS
Enable SIPS: Enable
SIP Destination Port: 5061

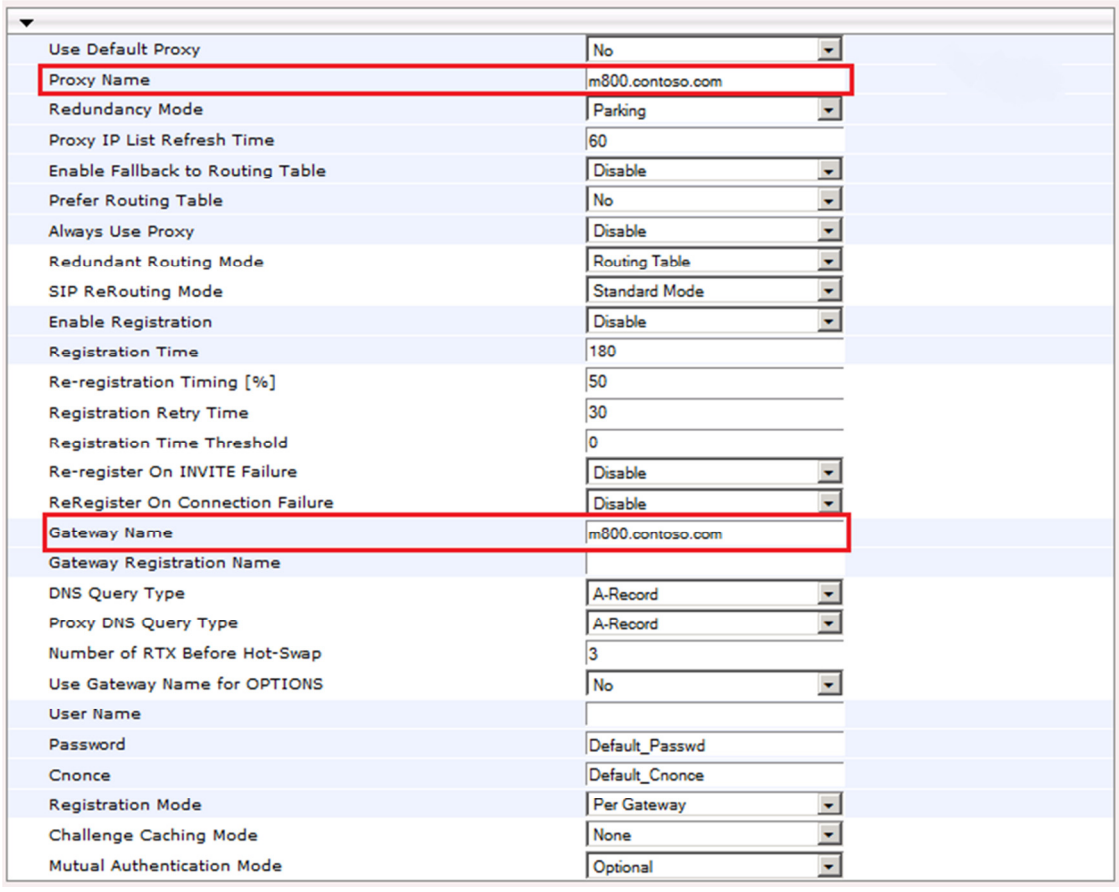

SIP General
NAT IP Address 0.0.0.0
PRACK Mode Supported
Channel Select Mode Cyclic Ascending
Enable Early Media Disable
183 Message Behavior Progress
Session-Expires Time 0
Minimum Session-Expires 90
Session Expires Method Re-INVITE
Asserted Identity Mode Disabled
Fax Signaling Method No Fax
Detect Fax on Answer Tone Initiate T.38 on Preamble
SIP Transport Type TLS
SIP UDP Local Port 5060
SIP TCP Local Port 5060
SIP TLS Local Port 5061
Enable SIPS Enable
Enable TCP Connection Reuse Enable
TCP Timeout 0
SIP Destination Port 5061
Use user=phone in SIP URL Yes
Use user=phone in From Header No
Use Tel URI for Asserted Identity Disable

25. Click **Submit**

26. Select **VoIP** > **SIP Definitions** > **Proxy & Registration**

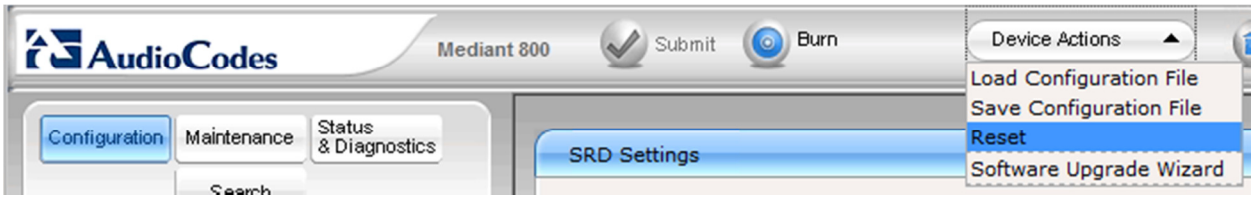


27. Enter the **Subject Name** used in generating the **CSR** in the **Gateway Name** & **Proxy Name** fields

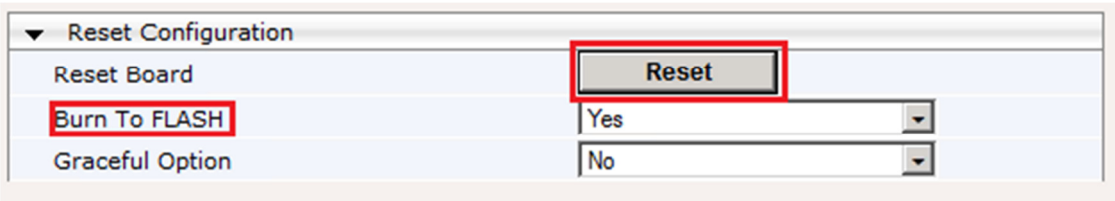

Use Default Proxy: No
Proxy Name: m800.contoso.com
Redundancy Mode: Parking
Proxy IP List Refresh Time: 60
Enable Fallback to Routing Table: Disable
Prefer Routing Table: No
Always Use Proxy: Disable
Redundant Routing Mode: Routing Table
SIP ReRouting Mode: Standard Mode
Enable Registration: Disable
Registration Time: 180
Re-registration Timing [%]: 50
Registration Retry Time: 30
Registration Time Threshold: 0
Re-register On INVITE Failure: Disable
ReRegister On Connection Failure: Disable
Gateway Name: m800.contoso.com
Gateway Registration Name:
DNS Query Type: A-Record
Proxy DNS Query Type: A-Record
Number of RTX Before Hot-Swap: 3
Use Gateway Name for OPTIONS: No
User Name:
Password: Default_Passwd
Cnonce: Default_Cnonce
Registration Mode: Per Gateway
Challenge Caching Mode: None
Mutual Authentication Mode: Optional

28. Click **Submit**

29. Select **Device Actions** > **Reset**



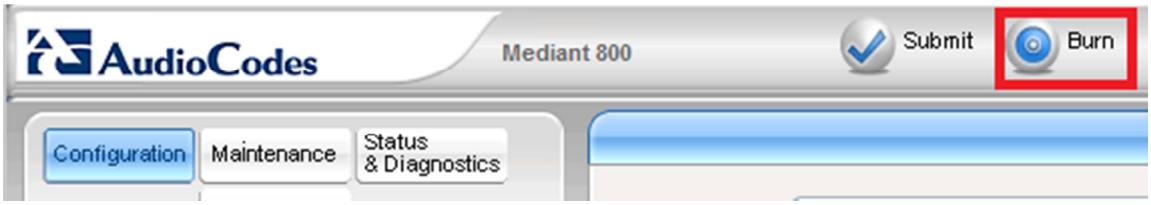
30. Ensure **Burn to Flash** is set to **Yes** and then click **Reset**



31. Log back in after reboot
32. Select **VoIP** > **Control Network** > **Proxy Sets Table**
33. Ensure that the proper proxy set has the **Transport Type** set to **TLS** for each entry in its **Proxy Address** table. Also put the **SIPS** communication port on the end of each IP Address.
34. If one of your proxy sets does not communicate using TLS ensure that that **Proxy Set** has the **SIP** communication port on the end of each of its **IP Addresses**.
35. Select **VoIP** > **Coders & Profiles** > **IP Profile Settings**

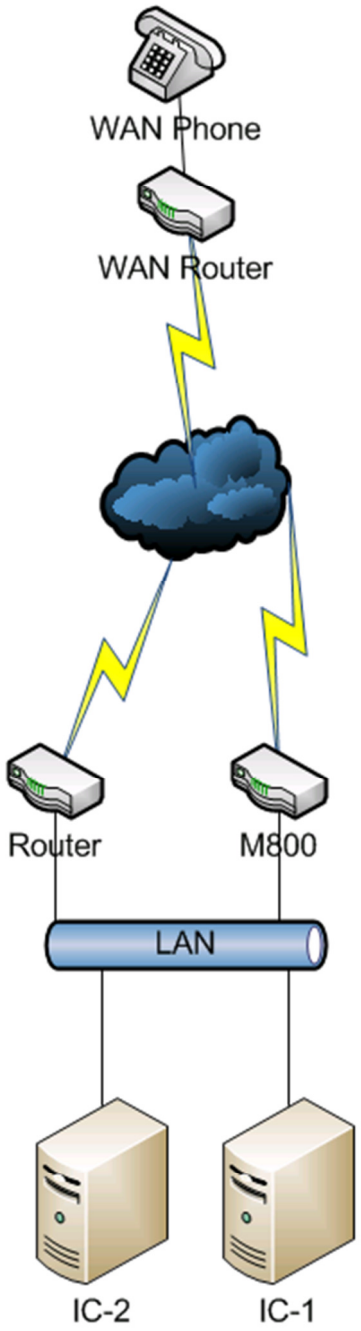
36. Create one **IP Profile** for **TLS** and one for **TCP/UDP**.
    a. For **TCP** set:
       Gateway Parameters > **Media Security Behavior** to **Disable**
       SBC > **Media Security Behavior** to **RTP**
    b. For **TLS** set:
       Gateway Parameters > **Media Security Behavior** to **Preferrable**
       SBC > **Media Security Behavior** to **SRTP**
37. Assign the **IP Profiles** to **IP Groups** as needed to control their Media Security behavior.
38. Click **Submit**

39. Click **Burn**



Advanced Installation – External User Agents:

If you wish to have VoIP stations outside your network that connect back to IC and place calls without using VPN there are several things you will need to configure. Primarily you cannot use the Mediant 800 for your primary Data router. You will instead need a Secondary router that will handle the HTTP(S) traffic from the WAN Phones. See the diagram below:



For IC to function properly with a WAN Phone & Switchover, all HTTP(S) traffic will need to be routed through a separate device than the M800. Ports 8088 and 8089 will need sent through your firewall using port forwarding, static NATs, or a separate method of your choosing.

The end result being that a WAN phone can contact either server for its configuration files, depending on which server is up at the time, and that the HTTP(S) traffic does not go through the M800.

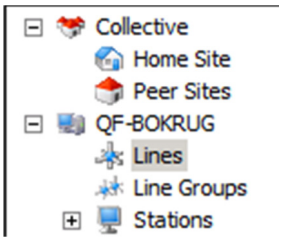
The reason for this is due to a limitation of the Mediant 800. If a DNS record returns more than one IP, the first IP returned is the only IP Address used.

One other thing to note is that this configuration disallows provisioning managed phones by end users, and rebooting the phones remotely. All phones will need their MAC addresses entered at time of creation.

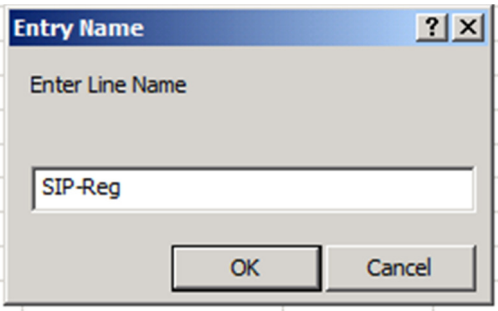
There will need to be several changes in Interaction Administrator before changes are made to the Mediant 800. There will need to be:

- A line for phones to register on, either 5060 or 5061 depending on the usage of TLS
- A registration group dedicated to WAN phones
- A location dedicated to WAN phones

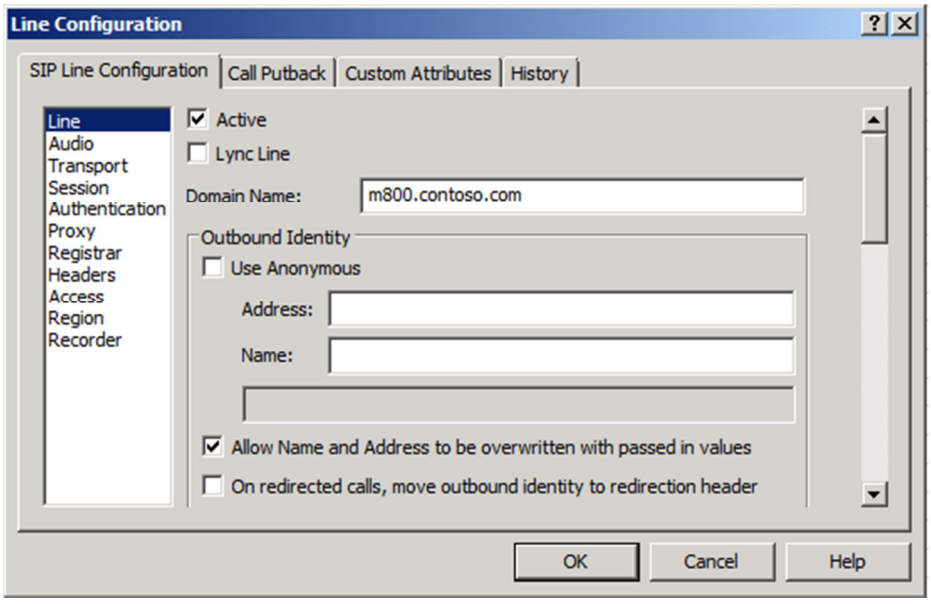
1. Open **Interaction Administrator** and navigate to the **Lines** Container



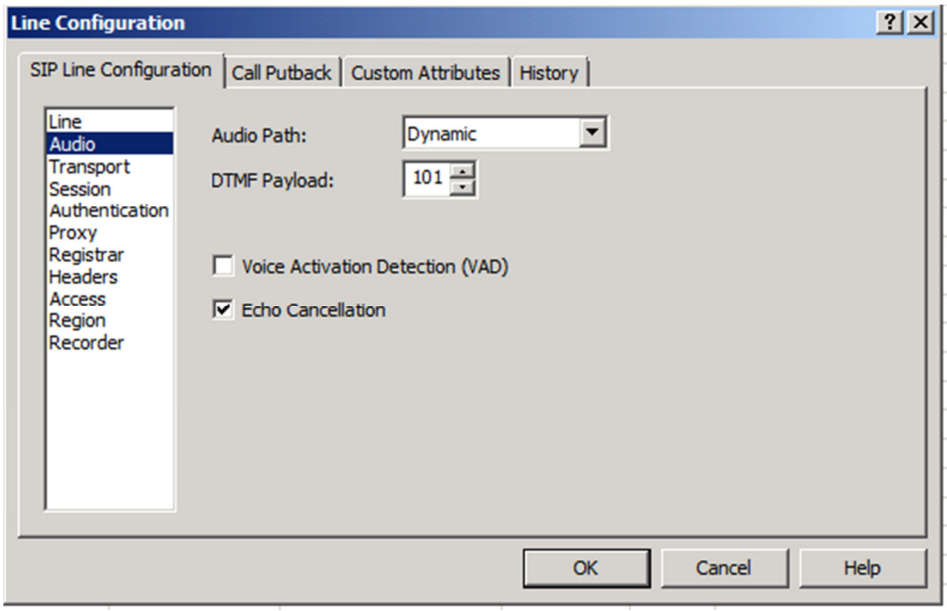
2. Click **File** > **New** and enter a meaningful name for the Line



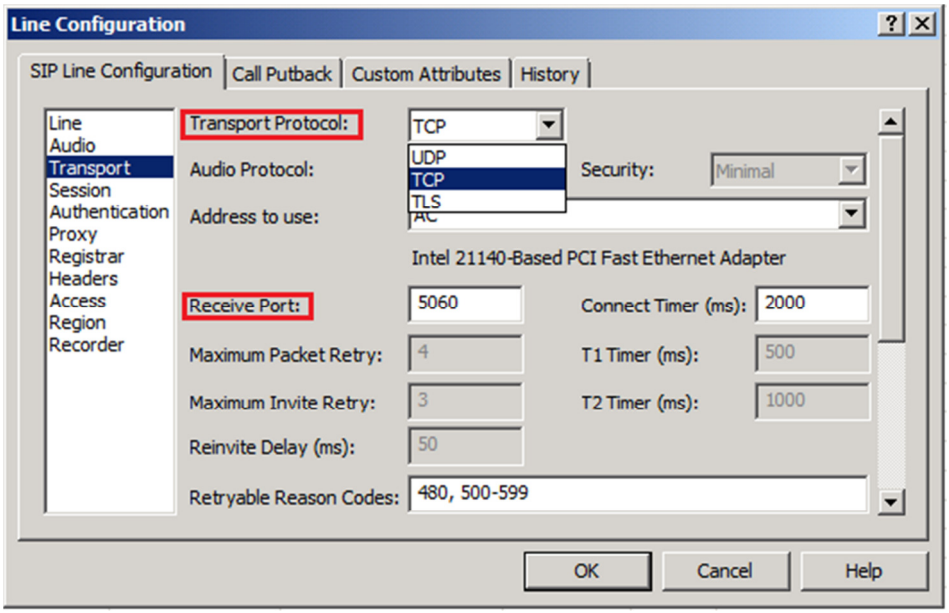
3. Enter the FQDN the WAN Phones will use to contact IC in the **Domain Name** field. Enter something in the **Address** field. This can be your main DID or another number.



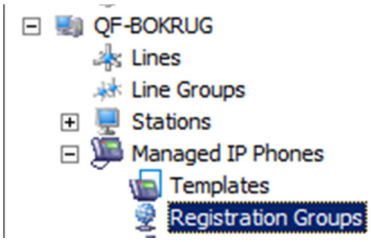
4. Change any settings necessary in the **Audio** section



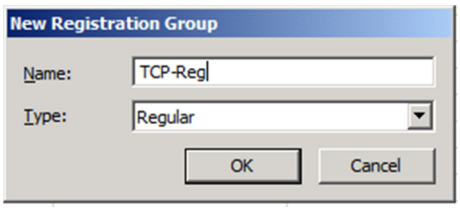
5. Change any settings necessary in the **Transport** section



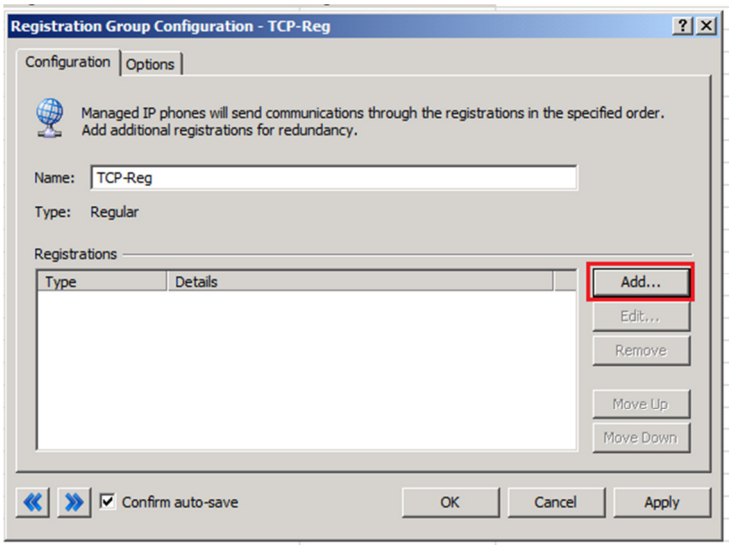
6. Click **OK**
7. Click **[Server Name]** > **Managed IP Phones** > **Registration Groups**



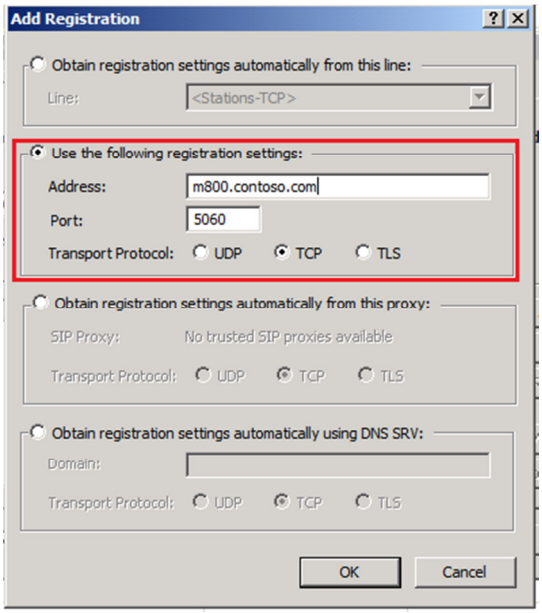
8. Click **File** > **New** and enter a name in the **New Registration Group** window



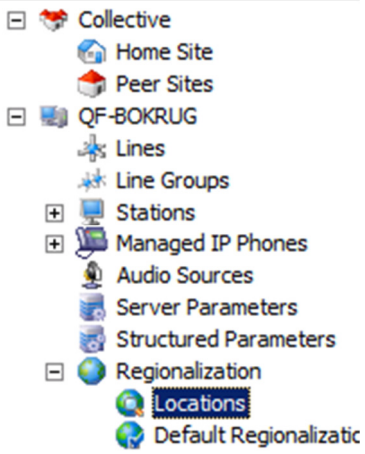
9. Click **Add..** in the **Registrations** section of the **Registration Group Configuration** window



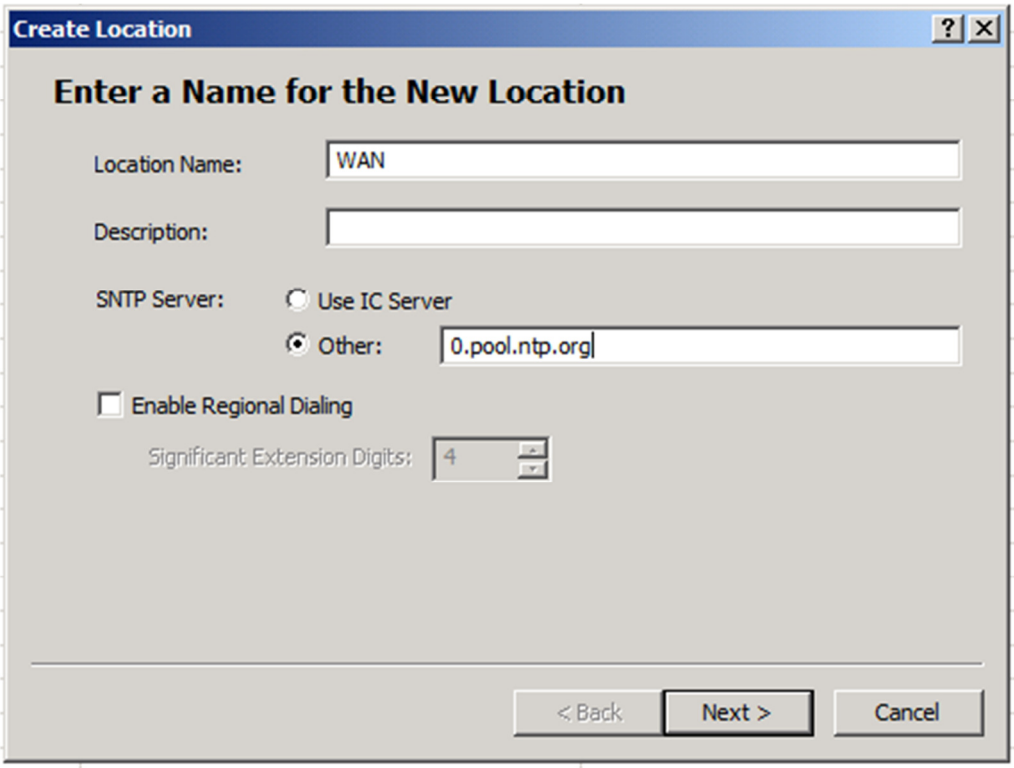
10. Click the **Use the following registration settings:** radio button.
11. Enter the external FQDN of your Mediant 800, the name entered in the **Subject Name** of the CSR, and change **Port** and **Transport Protocol** as necessary.



12. Click **OK**
13. Click **[Server Name]** > **Regionalization** > **Locations**

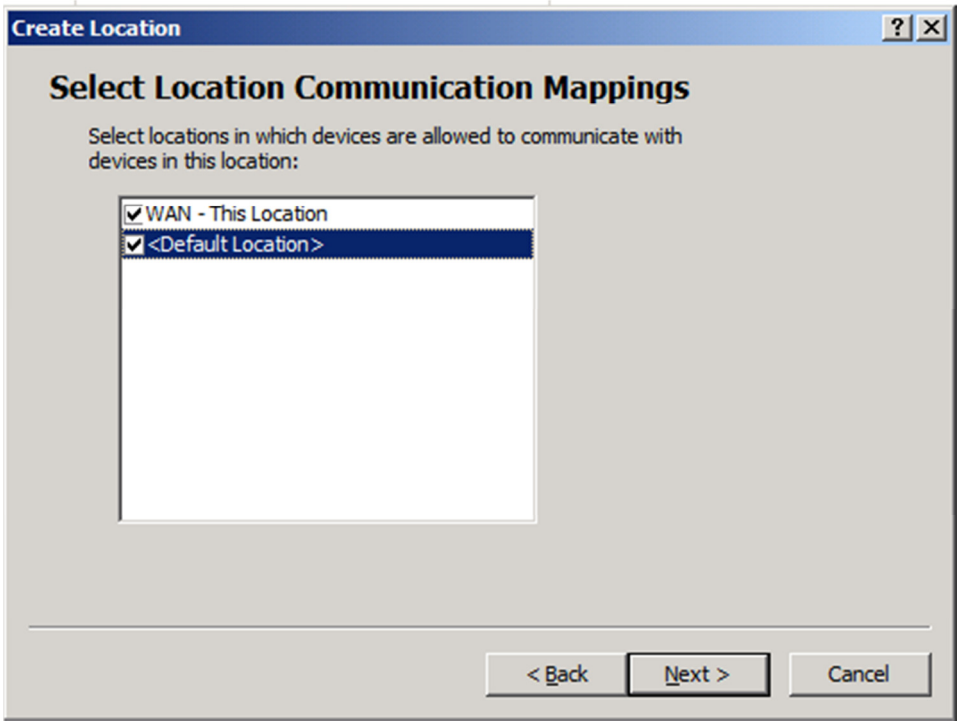


14. Click **File** > **New**
15. Enter a meaningful **Location Name** and, if there is no way to route NTP back to your network from the WAN, choose **Other** for **SNTP Server** and enter the IP or FQDN of a public NTP server.

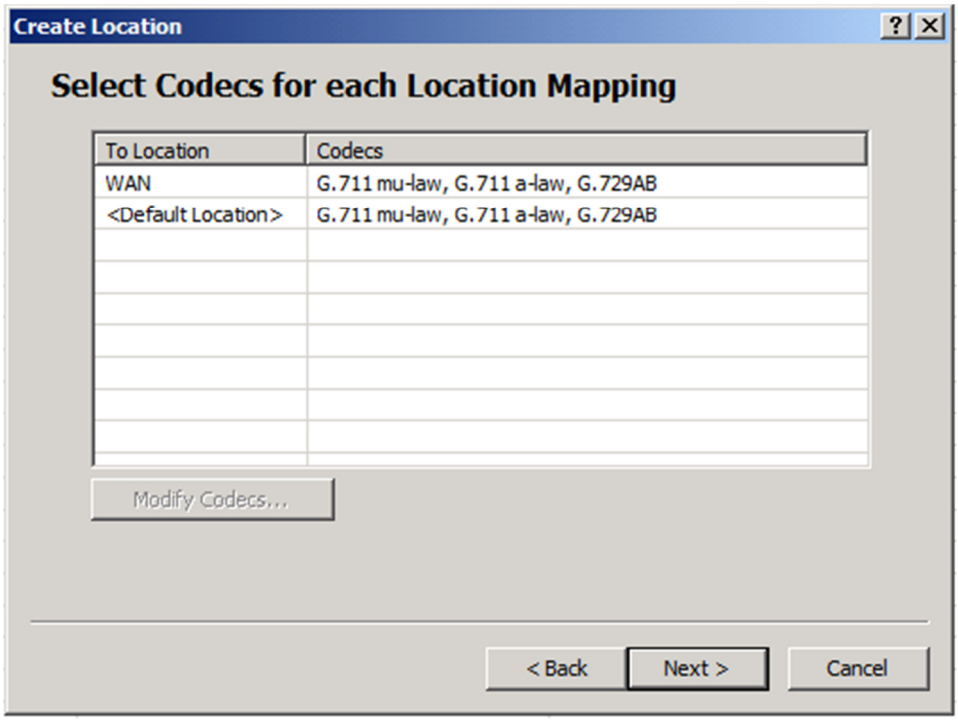


16. Click **Next**

17. Select the other **Location**(**s**) this **Location** needs to be able to communicate with



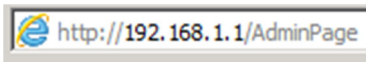
18. Click **Next**
19. Choose the **Codecs** available at each **Location**



20. Click **Next**
21. Click **Finish**

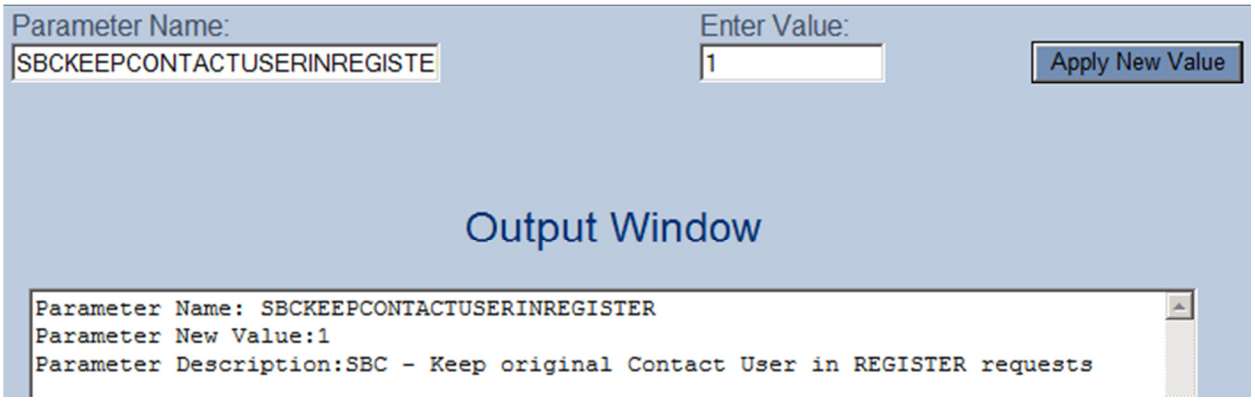
22. Create some Managed Phones/Stations and place them in the WAN region.

23. Open the Mediant 800's WEB Interface
24. Change the URL replacing **Index** with **AdminPage** (this is case sensitive)



25. Select ***ini* Parameters**

26. Enter **SBCKeepContactUserInRegister** in the **Parameter Name** field and **1** in the **Enter Value** field, click **Apply New Value**



27. Click **Back to Main** to return to the regular configuration page.

28. Select **VoIP** > **Control Network** > **IP Group Table**

29. Select **Index 12** and enter the following settings:

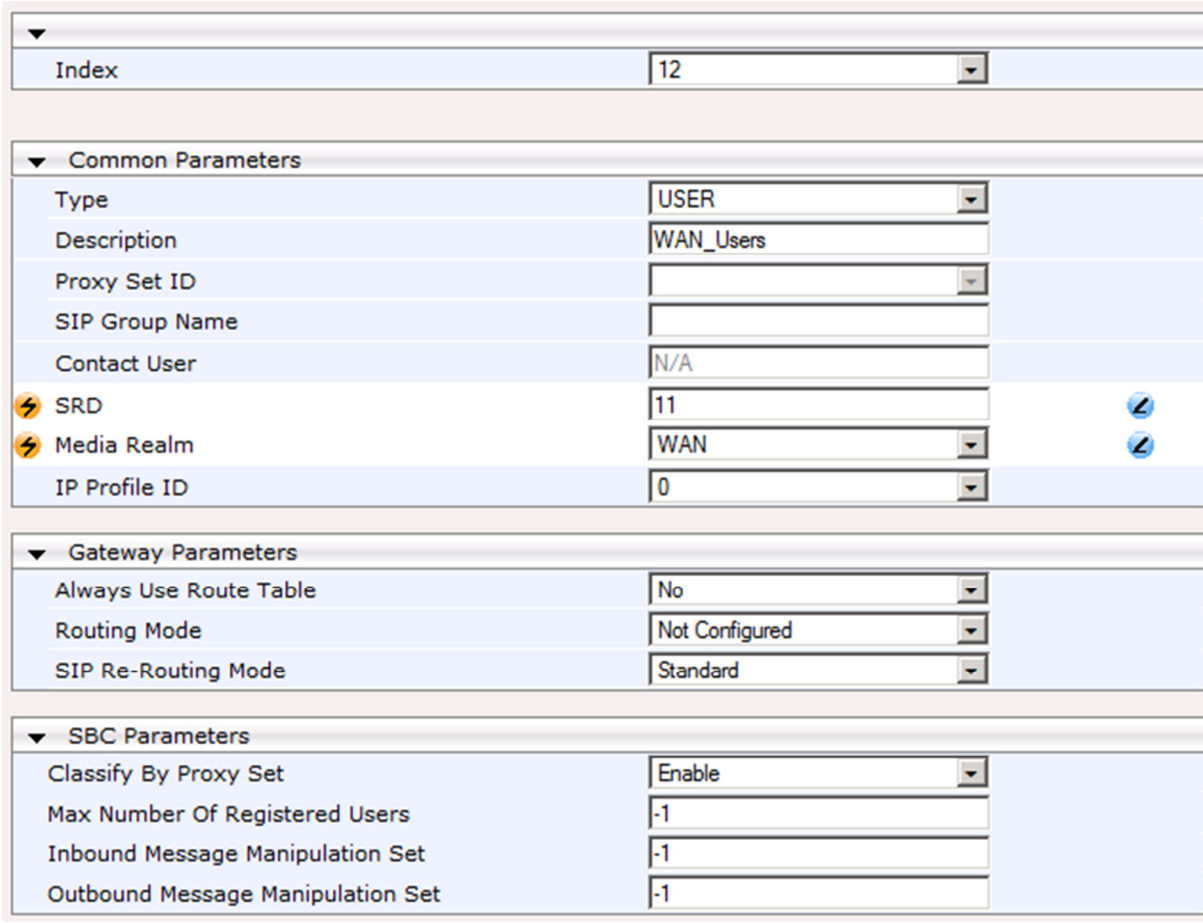
    Type: USER

    Description: WAN Users (or something more meaningful)

    SRD: 11

    Media Realm: WAN

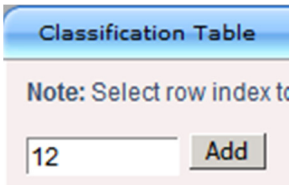
    IP Profile ID: Choose the appropriate IP Profile unless non used, then choose 0



30. Click **Submit**

31. Select **VoIP** > **SBC** > **Routing SBC** > **Classification Table**

32. Enter 12 in the text box next to **Add** and click **Add**

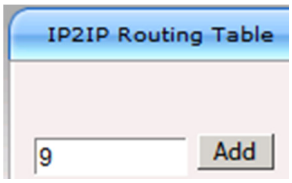


33. Enter
    a. **Source SRD ID**: 11
    b. **Source IP Group ID**: 12

34. Click **Apply**

35. Select **VoIP** > **SBC** > **Routing SBC** > **IP to IP Routing Table**

36. Enter a **9** in the box next to **Add**



37. Enter the following Settings:

Source IP Group ID: 1

Destination Username Prefix: WANPhoneXXX

i. A strict naming convention will have to adopted for all phones that are going to be on the WAN so that this naming mask will be effective.

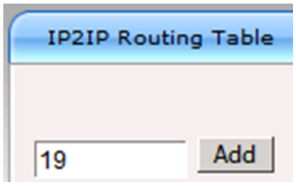
ii. This naming mask will handle any phone named WANPHONE(001-999) as X is wild card for a single digit 0-9.

Destination IP Group: 12

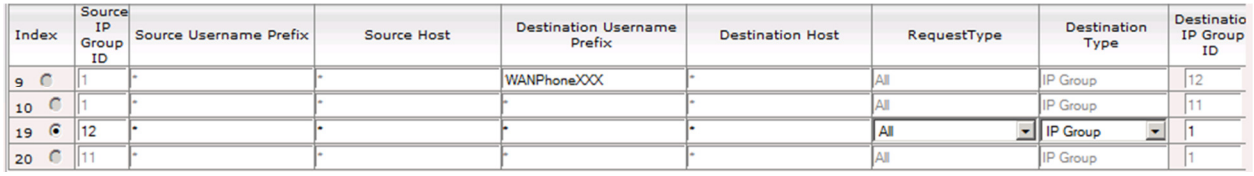
Index	Source IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	RequestType	Destination Type	Destination IP Group ID
9	1	*	*	WANPhoneXXX	*	All	IP Group	12
10	1	*	*	*	*	All	IP Group	11
20	11	*	*	*	*	All	IP Group	1

38. Click **Apply**

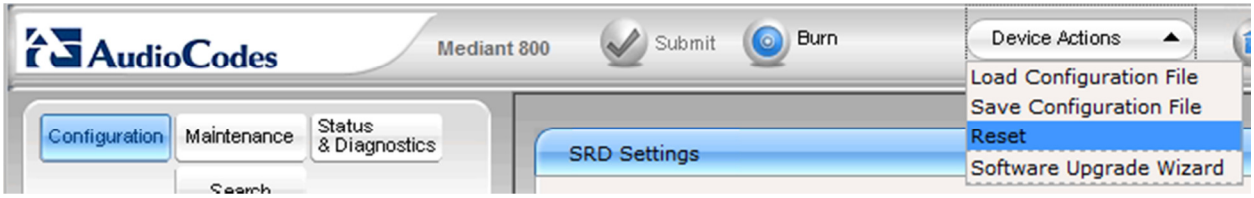
39. Enter a **19** in the box next to **Add**



40. Enter the following Settings:
    a. **Source IP Group ID**: 12
    b. **Destination IP Group**: 1


Index
Source IP Group ID
Source Username Prefix
Source Host
Destination Username Prefix
Destination Host
RequestType
Destination Type
Destinatio IP Group ID
9 1 * * WANPhoneXXX * All IP Group 12
10 1 * * * * All IP Group 11
19 12 * * * * All IP Group 1
20 11 * * * * All IP Group 1

41. Click **Apply**
42. Select **Device Actions** > **Reset**



43. Ensure **Burn to Flash** is set to **Yes** and then click **Reset**